Written Testimony of Tom Walker

Chief Executive Officer, DroneUp

House Committee on Homeland Security

Surveillance, Sabotage, and Strikes:

How Drone Warfare Abroad is Transforming Threats at Home

July 8, 2025

Introduction and Purpose

Chairman Gimenez, Ranking Member McIver, and Members of the Committee:

I am Tom Walker, Chief Executive Officer of DroneUp and a former U.S. naval officer. Throughout my career, from military service to leading one of the nation's largest uncrewed aviation networks, I have witnessed the rapid evolution of drone technology, both in its ability to serve the public and in the emerging risks it poses to national security.

My written testimony provides operational data and firsthand insights from thousands of commercial drone missions conducted across the United States. These missions have revealed consistent vulnerabilities in our airspace and infrastructure that warrant urgent attention from the federal government.

I will also outline practical measures that government and industry can take together to close these gaps, improve airspace coordination, and reduce the risks posed by uncrewed systems.

I appreciate the Committee's leadership on this issue and stand ready to support efforts to ensure the safety, security, and scalability of U.S. airspace.

Background and Qualifications

DroneUp was founded in 2016 to scale drone services nationwide. We built what became the world's largest drone services network, activating tens of thousands of independent drone pilots nationwide.

We subsequently launched the largest drone delivery operation in the country at that time, with the capacity to serve nearly four million households through partnerships with major retailers and state governments.

As part of that effort, we operated 34 drone hubs in six states, including Chairman Gimenez's home state of Florida. We obtained FAA Part 135 Air Carrier Certification and gained firsthand insight into both the operational potential and the technical limitations of drone systems at scale.

As our operations expanded, it became clear that the most significant constraint was not aircraft performance or logistics. The limiting factor was the absence of a technological foundation to safely integrate uncrewed systems into national airspace. Ensuring future aviation safety, protecting critical infrastructure, and maintaining safe separation between crewed and uncrewed aircraft requires a systems-level solution.

Today, DroneUp focuses on integrating autonomous airspace using AI-enabled technology. Our platform enables real-time deconfliction, autonomous flight coordination, and persistent situational awareness in dynamic and high-risk environments. We collaborate directly with federal regulators, defense agencies, and commercial operators to close security and operational gaps that traditional aviation systems were never designed to address.

This perspective is grounded in real-world operational experience and technical development. It reflects what we are already observing in the field and what must now be done to protect the airspace.

Overview of the Threat Landscape

As of mid-2025, the United States is facing a sharp escalation in drone-related threats across aviation, infrastructure, and national security. In the first quarter of 2025 alone, the FAA recorded 411 illegal drone incursions near U.S. airports, a 25.6 percent increase over the same period in 2024 (FAA).

Separately, U.S. Northern Command documented over 350 unauthorized drone flights across more than 100 military installations in 2024 (Fox News).

These are not isolated incidents. They are active, sustained, and growing. They disrupt flight operations, interfere with emergency services, and expose vulnerabilities at military and civilian facilities nationwide.

This is not a domestic problem alone. Internationally, drones have shut down major airports, penetrated secure sites, and been used for espionage, sabotage, and targeted attacks. When drone activity shut down London's Gatwick Airport for 33 hours in 2018, it disrupted 1,000 flights and stranded over 140,000 passengers (BBC). That type of disruption is no longer hypothetical here. It is beginning to happen on U.S. soil.

The threat is real, immediate, and growing faster than our ability to contain it.

Threats to Aviation

Drones now pose a direct and rising risk to manned aviation in the United States. In 2024, they accounted for nearly two-thirds of all reported near mid-air collisions at the nation's 30 busiest airports, according to analysis by the Associated Press and NASA's Aviation Safety Reporting System (AP News, The Sun).

Pilots have reported drones within hundreds of feet of commercial aircraft during takeoff and landing:

- A quadcopter flew within 300 feet of a jetliner's cockpit on approach to San Francisco International (AP News)
- A drone was observed at 4,000 feet near Miami International
- At Newark Liberty, a drone came within 50 feet of a departing jet's wing

The FAA continues to receive over 100 drone sighting reports every month near U.S. airports (FAA).

The trend is accelerating, and these are not all near misses. In January 2023, an F-16 fighter jet collided midair with a drone during a training mission over Arizona (AZFamily). In January 2025, a drone struck a Los Angeles County firefighting aircraft during an emergency evacuation, tearing a 6-foot hole in the wing and grounding the aircraft while 192,000 residents were under evacuation orders (ABC7, AP).

The threat is global. In September 2023, a Virgin Atlantic Boeing 787 carrying 264 passengers narrowly avoided a drone collision just after takeoff from Heathrow Airport. U.K. aviation authorities described it as one of the closest calls on record (D-Fend Solutions).

Many of these drones are too small to appear on radar and are often operated by individuals who may not be visible to authorities. Without stronger detection systems, improved coordination, and apparent enforcement authority, the risk to commercial and emergency aviation will continue to grow.

Threats to Critical Infrastructure

Military Installations

Drone incursions into U.S. military airspace have reached unprecedented levels. In December 2023, Langley Air Force Base in Virginia experienced 17 consecutive nights of drone overflights. Witnesses described formations as large as 20 feet long, traveling at 100 miles per hour, and reaching altitudes of 3,000 to 4,000 feet (Task & Purpose). The incident forced the relocation of F-22 Raptor aircraft and the suspension of training operations. Despite weeks of investigation by the Pentagon, FBI and NASA, the drone operators were never identified.

In December 2024, Wright-Patterson Air Force Base was forced to close its airspace for four hours due to heavy UAS activity. Controllers reported multiple unidentified drones operating over the facility (CNN, The War Zone).

These are not hobbyist drones. These are sustained, strategic incursions targeting sensitive national security infrastructure.

Energy Infrastructure

In 2024, over 13,000 drone incursions were detected at U.S. power generation sites. Analysts estimate that 60 new vulnerability points are added to the grid every day (E&E News, Dedrone). The Department of Homeland Security has warned that extremist actors and foreign adversaries have considered using drones for surveillance or sabotage.

In January 2024, the Cybersecurity and Infrastructure Security Agency and the FBI issued a joint advisory warning that Chinese-manufactured drones operating in the U.S. energy and telecommunications sectors could expose sensitive data to foreign access (CISA).

Prisons

Drones are now a standard tool for delivering contraband into U.S. prisons. From 2023 to 2024, Georgia reported 774 drone sightings at state correctional facilities. Of these, 720 involved contraband drops, including drugs, weapons, and cellphones. The incidents led to over 540 felony arrests. At Washington State Prison alone, authorities intercepted 21 drone drops in one year, arresting more than 40 individuals linked to smuggling operations (WGXA News).

Public Events

In 2023, NFL stadiums reported 2,845 unauthorized drone incursions, up from just 67 in 2018, a 4,145 percent increase (Reuters). The NFL, Department of Justice, and FBI have all called on Congress to expand detection and mitigation authority to protect public events.

Ports and Maritime Infrastructure

America's maritime transportation system underpins more than $5.4 trillion in economic activity and carries over three-quarters of all U.S. trade, according to the 2023 Cyberspace Solarium Commission and independent StateScoop reporting. (cybersolarium.org, statescoop.com)

Yet ports remain attractive, under-protected targets. The Port of Los Angeles blocked roughly 60 million attempted cyber-intrusions every month in 2023, up from 7 million in 2014, its chief information-security officer told trade press and security researchers. (ajot.com, amu.apus.edu)

At the same time, the U.S. Coast Guard warns that unauthorized drone flights over sensitive maritime facilities have become “a common occurrence,” and that most local authorities still lack the equipment and legal authority to detect or interdict them. (hstoday.us)

These low-cost aircraft can hover above container stacks, record ship movements, and capture other line-of-sight intelligence that traditional perimeter systems cannot block, exposing a critical gap between the economic value of U.S. ports and the security resources dedicated to protecting them.

Conclusion: A Growing Gap Between Threat and Response

These incidents are not anomalies. They reflect an accelerating pattern. Drone technology is becoming faster, cheaper, and easier to operate, while our detection systems, legal authorities, and response capabilities have not kept pace. From airliners and emergency aircraft to power grids, prisons, and ports, drones are exposing fundamental operational gaps.

If these vulnerabilities are not addressed with urgency and coordination, it is not a matter of if they will be exploited, but when and with what consequence.

The System We Were Promised Still Doesn’t Exist, and the Gap Is Dangerous

By 2017, NASA’s UTM trials had demonstrated that data-driven services, rather than radio calls, could safely manage low-altitude drones. The industry told Congress that a nationwide system was imminent. Every drone would file a digital plan, receive near-instant clearance, and broadcast a trusted ID while shielding crewed aircraft and sensitive airspace.

Eight years on, that promise remains unfulfilled. LAANC automates only the simplest flights; Remote-ID is little more than a broadcast license plate; and the architecture intended to weave

authorization, intent, surveillance, and enforcement into a single safety net stalled at the prototype stage. The low-altitude NAS is a patchwork of manual waivers, siloed registries, partial awareness, and policy-only defenses.

Nine critical gaps keep the system fragmented:

1. **Patchwork Authorization** – Anything beyond basic flights slides into slow waivers; approval pipelines don't share live pilot, aircraft, or risk data, so regulators default to broad caps no one can enforce.

2. **Fragmented Identity** – Pilot certificates, hull IDs, Authorizations, and Restrictions all live in different databases. Nothing cryptographically binds drone + pilot + mission.

3. **No Live Intent Ledger** – While each DSS can expose only minimal "need-to-know" metadata, each USS keeps its complete plans private. Multiple DSSs can overlap but federate only on a best-effort handshake, with no cryptographic trust anchor or shared governance in place. The result: no authoritative, real-time ledger of intent, leaving controllers, law enforcement, and defense without a complete situational picture or conformance guarantee.

4. **Prototype-level UTM Functions** – While basic constraint ingestion has been proven, functions such as collaborative detect-and-avoid, demand/capacity balancing, and dynamic rerouting remain at the prototype stage, even as low-altitude drone activity continues to rise faster than the supporting infrastructure can keep pace.

5. **Policy-only Protection** – Flight rules, TFRs, and NOTAMs depend on voluntary compliance. The 2018 Gatwick shutdown demonstrated how quickly policy can fail when

authorities can't verify or neutralize a rogue drone. The recent withdrawal of manufacturer geofences further widens the exposure.

6. **Thin Cooperative Detection** – Remote-ID has a limited range, can be spoofed, and has experienced slow adoption; significant gaps exist in conformance validation and law enforcement's ability to respond.

7. **Invisible Manned Traffic** – ADS-B Out is mandatory only in controlled cores. Below 10,000 ft or outside Mode C veils, numerous helicopters and general aviation aircraft fly electronically dark. Drones must either hire human spotters or stay grounded, while manned pilots receive no warning, creating an asymmetric blind spot that endangers safety and national security.

8. **Siloed Non-cooperative Sensors** – Radar, RF, acoustic, and EO/IR feeds terminate in siloed consoles. Without a consolidated fusion layer that de-duplicates tracks, tags provenance, and applies confidence scores, agencies lack an authoritative air picture; low-signature threats slip through the seams while false alarms drain resources.

9. **Minimal Enforcement Tools** – Many agencies lack the resources, statutory authority, or training to act; penalties rarely deter non-compliance.

These gaps compound: the labyrinthine nature of authorizations, weak identity, a missing intent ledger, and endless prototype tests and deployments have left the NAS blind. Policy-only protection and scant enforcement embed risk; asymmetric conspicuity and unfused sensors hamper both safety and security. Domestic incidents, from prison contraband drops to critical‑infrastructure overflights, are accelerating, and foreign actors already field swarm‑scale, AI‑directed drone operations that would overwhelm today's fragmented defenses.

Without a fully digital, interoperable, security-grade low-altitude traffic management and security backbone, we risk ceding safety, commerce, and strategic credibility. Closing these gaps requires a cohesive national program. One that unifies real-time authorization and intent data, provides universal e-conspicuity for every aircraft, fuses cooperative and non-cooperative sensor feeds, and ensures adequately funded enforcement and training, so that every flight is known, every risk is quantified, and every violation is actionable.

Building a Safe, Trusted, and Scalable Low-Altitude Airspace

What we need today is not theoretical. It is practical, achievable, and urgent. The foundation is simple. If something is in the sky, we should know what it is, who is operating it, whether it belongs there, and how to respond if it does not.

Establish a National Low-Altitude Information & Flight Exchange

The exchange will provide every UAS Service Supplier and government stakeholder with a live, sub-second view of low-altitude airspace by requiring them to publish their flight data to, and subscribe to, a common event bus protected by role-based access control. An immutable, cryptographically signed ledger will preserve each transaction, enabling regulators, first responders, and counter-UAS systems to verify provenance and reconstruct events with forensic certainty.

Deploy a Unified Flight-Authorization Service

This service will replace disparate grids, waivers, and letters of authorization with a single standards-based API. Operators will submit an Operational Intent that describes their mission and objectives. The service will automatically validate airspace status, aircraft performance, crew credentials, and relevant exemptions, and then issue a digitally signed authorization token. The token will be broadcast via Remote-ID during flight and stored in the National Low-Altitude

Information and Flight Exchange, providing field personnel with instant compliance checks and enabling the FAA with a tunable, permission-verified control point for all mission types.

Mandate Digital Credentials & Binding

Verifiable credentials will cryptographically bind pilot, aircraft, flight plan, and authorizations. Any mismatch or change in authorization will block take-off and trigger immediate alerts. Public-safety officers will resolve a Remote-ID signal to a licensed operator with one query, and insurers will rely on tamper-evident evidence after an incident.

Require Universal Electronic Conspicuity

All crewed and uncrewed aircraft will transmit a verifiable position signal using onboard equipment or low-power beacons. Making every aircraft electronically visible balances the see-and-avoid burden and enables safe, scalable drone operations nationwide.

Implement Network Remote-ID & Non-Repudiation

Add a compact cryptographic signature to every Remote-ID packet, broadcast or online, so the Unified Flight-Authorization Service, public-safety observers, and counter-UAS sensors can verify authenticity within milliseconds. Spoofed or replayed identifiers will be flagged instantly, while genuine packets will flow unchanged into the National Low-Altitude Information & Flight Exchange as tamper-proof evidence. Every legitimate drone in U.S. airspace will thus carry a verifiable, non-repudiable identity, providing regulators, integrators, and first responders with the cryptographic certainty needed to automate trust decisions at machine speed.

Adopt a Mission-Priority Rules Engine

Embed a five-tier priority framework directly in the authorization service so emergency, public-safety, and critical-infrastructure flights automatically outrank commercial and recreational missions. The engine will eliminate manual deconfliction and restore predictability

for time-sensitive operations.

Build a Sensor-Fusion Backbone for Low-Altitude Surveillance

Fuse cooperative tracks from the National Low-Altitude Information & Flight Exchange with radar, RF, acoustic, and electro-optical detections provided by government and commercial sources. Privacy controls will permit graduated data disclosure, ensuring that all authorized users, from airport towers to local law enforcement, use the same trusted, continuously updated common operating picture.

Launch a Friend-or-Foe API

Provide authorized sensors and effectors with a one-call verdict: COMPLIANT, UNKNOWN, or HOSTILE, plus confidence and priority metadata. This API will shorten decision cycles, reduce friendly-fire risk, and log every query for after-action accountability.

Operate a Flight-Restricted-Area Service

Publish a single, near-real-time catalog of restricted airspace, § 2209 critical-infrastructure sites, stadium Temporary Flight Restrictions, wildfire boxes, VIP security rings, and temporary counter-UAS volumes, and push updates digitally within seconds. The authorization service will validate the current catalog during planning and periodically in flight. If a change is detected, onboard logic will force a reroute or a safe landing, delivering geofence-like protection in a standardized, manufacturer-agnostic format.

Fund a Local-Enforcement Equip-and-Train Program

Supply state, local, tribal, and territorial agencies with multi-band Remote-ID receivers tied into the National Low-Altitude Information & Flight Exchange, a Friend-or-Foe–enabled mobile application, and concise online training. Statutory amendments will authorize certified officers to order landings or seize non-compliant aircraft, transforming federal data streams into actionable

local enforcement.

Start a Vehicle-to-Vehicle Spectrum & Standards Initiative

Kick off a technical and regulatory effort to identify and allocate low-latency spectrum for direct detect-and-avoid messaging between crewed and uncrewed aircraft, while deferring any equipage mandate until the Unified Flight-Authorization Service and Universal Electronic Conspicuity have operated long enough to reveal any remaining mid-air-collision risk.

Why Time is Critical

The pace of the drone threat is outstripping our national response. What was once a future-looking concern is now a present and growing danger. The volume, complexity, and frequency of drone-related incidents are rising across every major sector: commercial aviation, military installations, public infrastructure, law enforcement operations, and emergency services. Each passing month adds to the evidence that we are operating in a risk environment that is evolving faster than our laws, technologies, and authorities can keep up.

This urgency is not abstract. It is measurable in hard numbers and operational strain. In the first quarter of 2025 alone, drone incursions near airports increased by more than 25 percent compared to the previous year. Security officials at military bases are now forced to treat drone sightings as recurring operational threats rather than one-off anomalies. Emergency response aircraft have been grounded mid-mission. Correctional facilities and utility providers are managing not theoretical vulnerabilities, but routine airspace violations.

What makes the current threat especially urgent is that many of the most critical policy tools to address it already exist on paper, but have not been implemented. For example, FAA Section 2209, mandated initially in 2016, was intended to create a process for restricting drone flights

over critical infrastructure. Nearly nine years later, the rule remains unfinalized, leaving power plants, refineries, and other sensitive sites without the reliable federal protection they need.

Similarly, the FAA's long-awaited rule to enable beyond visual line-of-sight (BVLOS) drone operations remains delayed. This rule is essential not only for commercial expansion but also for ensuring the safe and scalable use of drones in emergency response and infrastructure monitoring. Its continued absence has created both operational inefficiencies and potential safety risks.

Most concerning is the limited authority for detecting and neutralizing rogue drones. As of today, only a handful of federal agencies have narrowly defined counter-UAS mitigation authority. State and local law enforcement, as well as most infrastructure operators, remain legally barred from using even basic mitigation tools. Bipartisan proposals to expand this authority have been repeatedly drafted, but Congress has yet to act. If the current federal authority sunsets in September 2025 as scheduled, no agency, federal or local, will have a clear legal ability to respond to a malicious drone in real-time.

We are approaching a point where the probability of a serious incident, such as a downed aircraft, a disrupted power grid, or a mass evacuation triggered by an airspace breach, is no longer low. Without coordinated action, the current patchwork of regulations and capabilities will leave critical gaps that adversaries, criminals, or careless actors can continue to exploit.

The United States has the technological capacity to lead in the safe and secure integration of drones. But every delay in closing these policy and infrastructure gaps increases the risk to public safety and national security. Time is not neutral. Inaction allows the threat to mature, while preparedness becomes more difficult and costly.

We are not sounding the alarm in anticipation of a future crisis. We are responding to the reality that the crisis has already begun. The question before us is how quickly we choose to act.

Conclusion and Call To Action

The vulnerabilities outlined in this testimony are not theoretical; they are real and present a significant risk. They are documented, active, and growing. The threats posed by uncrewed aerial systems to aviation safety, critical infrastructure, and national security have increased in frequency, complexity, and impact. At the same time, the systems designed to detect, identify, authorize, and respond to these threats remain fragmented, underdeveloped, and in many cases unenforced.

The foundational technologies required to close these gaps are already available. Real-time airspace coordination, digital flight authorization, cryptographically verifiable credentials, secure identity broadcasts, and integrated sensor fusion are not experimental. These capabilities have been demonstrated in operational environments and validated through collaboration between government and industry. What remains is the directive to implement them at scale.

To that end, I respectfully submit the following priorities for immediate Congressional action:

1. **Mandate the establishment of a national real-time low-altitude airspace coordination framework.** This system must integrate flight intent, identity, and enforcement data into a single operational platform.

2. **Require digital credentialing that binds pilots, aircraft, missions, and authorizations.** This will enable instant validation of lawful flights and allow for automated detection of non-compliant activity.

3. **Implement a universal electronic conspicuity requirement for all crewed and uncrewed aircraft operating below 18,000 feet.** This is essential for ensuring visibility and reducing the risk of mid-air collisions.

4. **Finalize FAA Section 2209 and direct the creation of a federal flight-restriction service.** This service must provide a machine-readable feed that all drones and autopilot systems consult before and during flight.

5. **Expand counter-UAS detection and mitigation authority to qualified state, local, tribal, and territorial agencies.** Oversight and safeguards must be in place, but these agencies need the authority to act.

6. **Fund and deploy a local law enforcement equip-and-train program.** This program must provide officers with the tools, training, and legal clarity to verify and respond to drone threats in the field.

7. **Require the FAA to implement a unified flight authorization service.** This service should support all drone operations through a single digital process from request to real-time verification.

Each of these actions addresses a core structural weakness that has allowed unregulated drone activity to outpace national preparedness. These are not isolated or speculative risks. They are recurring incidents that have grounded emergency aircraft, disrupted commercial aviation, penetrated military airspace, and exposed key infrastructure to surveillance and interference.

The timeline for addressing these issues is urgent. As the pace of drone innovation continues to increase, so does the risk of a high-consequence event. The United States cannot afford to treat

low-altitude airspace as an ungoverned or optional domain. It must be protected with the same level of accountability and structure applied to every other mode of transportation that affects public safety and national defense.

Congress has both the authority and the responsibility to ensure this system is put in place. The tools are ready. The risks are known. The solution is feasible. What is needed now is coordinated direction and the will to act.

I thank the Committee for the opportunity to provide this written testimony. I stand ready to support any effort that will help secure the national airspace system and enable the safe, scalable, and responsible integration of uncrewed aircraft systems in the United States.

Respectfully submitted,

Tom Walker

Chief Executive Officer, DroneUp