MARK E. GREEN, MD, TENNESSEE
CHAIRMAN

BENNIE G. THOMPSON, MISSISSIPPI
RANKING MEMBER

One Hundred Nineteenth Congress
Committee on Homeland Security
U.S. House of Representatives
Washington, DC 20515

Tuesday, July 15, 2025

10:00 a.m. EDT in 310 Cannon House Office Building

Subcommittee on Transportation and Maritime Security

Hearing

"Surveillance, Sabotage, and Strikes: Industry Perspectives on How Drone Warfare Abroad Is Transforming Threats at Home"

WITNESSES

Mr. Church Hutton
Chief Growth Officer
AeroVironment, Inc.

Mr. Tom Walker
Founder & CEO
DroneUp

Mr. Brett J. Feddersen
Vice President
Strategy & Government Relations
D-Fend Solutions

Mr. Michael Robbins
President & Chief Executive Officer
Association for Uncrewed Vehicle Systems International

Brett Feddersen
Vice President for Strategy and Government Affairs
D-Fend Solutions AD, Inc.

BEFORE

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Transportation and Maritime Security

HEARING ENTITLED

Surveillance, Sabotage, and Strikes: Industry Perspectives on How Drone Warfare Abroad Is Transforming Threats at Home

ON

July 8, 2025
Washington, DC

INTRODUCTION

Chairmen Gimenez and Green, Ranking Members McIver and Thompson, and distinguished members of the Subcommittee, thank you for the opportunity to testify before you on matters critically important to the national security and public safety of our country and its citizens.

My name is Brett Feddersen, and I am the Vice President of Strategy and Government Affairs at D-Fend Solutions, the leading counter-drone manufacturer of radio frequency (RF)-cyber takeover solutions for the drone threat, both overseas and in the United States. I also serve as the Chair of the Security Industry Association's (SIA) Drone Security Subcommittee and have been working on the drone and counter-drone problem set since 2008, during my time in the military, as a federal civilian, and in the private sector. Today, I am honored to appear before the Subcommittee representing both D-Fend Solutions and the drone security industry.

Bottom line up front: Drone warfare abroad has evolved rapidly over the past decade, with state and non-state actors fielding drones for surveillance, sabotage, and strikes in theaters from Eastern Europe to the Middle East. Tactics refined in these conflict zones—persistent reconnaissance, weaponized loitering munitions, and saturation swarm attacks—are now manifesting as emerging threats to U.S. homeland and national security.

These threats are here to stay and mean that things like our critical infrastructure—such as power grids, water treatment plants, transportation networks, and communication systems—is increasingly vulnerable to threats from nefarious actors who can exploit drones' capabilities, including surveillance, sabotage, and payload delivery, to conduct physical attacks. Successful drone attacks on critical infrastructure can lead to power outages, transportation disruptions, communication failures, and substantial economic consequences. More concerning is the potential for the loss of human life, for example, a drone using aerosol dispersal or payload delivery over a mass gathering can cause mass panic, causing serious injury or even death to attendees. Confronting this reality requires a proactive and multi-layered homeland defense strategy that includes early detection, safe and effective mitigation technologies, and updated security protocols.

From local football games to open-air shopping centers, large gatherings of Americans are part of our everyday lives and remain incredibly vulnerable to drone-based threats. As the United States prepares to host high-profile, global sporting events like the 2026 FIFA World Cup and the 2028 Olympics, I am grateful that the Committee is closely overseeing the threat environment and preparations for these events and is willing to engage in difficult conversations surrounding our real vulnerability and capability gaps.

Today, I hope to help the Subcommittee better understand how overseas drone operations are transforming domestic risk vectors, the status of U.S. capabilities and legal frameworks, and offer targeted recommendations for Congress to bolster detection, interdiction, and resilience against drone-borne threats in the United States homeland.

MODERN DRONE WARFARE ABROAD AND AT HOME

Drones have transitioned from niche reconnaissance tools to central components of modern warfare. Their wide availability, small size, low cost, and modular payloads make them attractive for intelligence, surveillance, and reconnaissance missions, as well as the destruction of critical infrastructure and the effective delivery of ordnance.

Just weeks ago, the world witnessed a historic shift in small drone warfare. Ukraine's planning and execution of Operation Spider Web has rewritten the rulebook on drone threats: distance, cost, and autonomy no longer constrain adversary reach. Below are key counter-drone lessons drawn from Ukraine's Operation Spider Web—an audacious campaign in which Ukraine struck Russian airbases up to 5,000 km (3,106 miles) from the front using small, commercial AI-enabled drones. This is farther than driving from New York City to Los Angeles.

- *Rear Areas Are Not Safe*
  Ukraine proved that "strategic depth" offers no immunity: drones launched from deep inside friendly territory reached ostensibly secure Russian airfields, destroying billions of dollars' worth of aircraft. Defenders must extend coverage well beyond the frontlines to include logistics hubs, maintenance depots, and forward operating bases.[1]
- *Defense in Depth—Layer Every Segment*
  Traditional point-defense systems (e.g., local radar or a single interceptor battery) were overwhelmed. Operation Spider Web integrated covert logistics, telecom exploitation, and ground infiltration to bypass singular defenses, underscoring the need for a layered approach to counter-drone detection (RF, radar, EO/IR) and mitigation (RF cyber takeover, electronic warfare measures, and directed energy).[2]
- *Resilience to Jamming and GPS Denial*
  Spider Web's drones used dead-reckoning navigation and civilian cellular (SIM-card) links rather than GPS, making them resilient to traditional GNSS jamming. Given this, counter-drone systems should include extensive RF spectrum monitoring, non-GPS-dependent geofencing, and safe mitigation techniques that can detect, take control of, or disrupt alternate control channels

In conflicts outside the U.S., inexpensive, commercially available, and do-it-yourself (DIY) drones have become the weapon of choice. Alarmingly, these same drones are flown across the U.S. every day. There are over one million drones registered with the FAA in the United States—a number that is predicted to grow to 2.7 million by 2027.[3]

The weaponization of private drones in the United States is a significant and growing concern. While drones have beneficial applications in public safety and various industries, their potential for misuse, especially when armed, poses challenges for law enforcement and national security. Battlefield tactics, techniques, and procedures for drones have proliferated through the internet, and the same drones used in combat overseas are available and in use here in the U.S.

During my time at the Federal Aviation Administration (FAA), we received several videos and briefings showcasing drones outfitted with chainsaws, flamethrowers, firearms, and makeshift chemical dispersal systems. We have witnessed rocket-propelled grenades (RPG) warheads and grenades being dropped from simple commercial and do-it-yourself (DIY) drones. Additionally, we have seen drones equipped with modified shotguns used to shoot down other drones.

[1] American University, "Ukraine's Operation Spider Web Upended Traditional Rules of War," June 5, 2025. Benjamin Jensen; chathamhouse.orgamerican.edu
[2] Counter-UAS Hub, "Putting Operation Spider's Web in Context," June 20, 2025, Ben Connable; cuashub.comirregularwarfare.org
[3] FAA, "Drones by the Numbers," updated April 1, 2025, https://www.faa.gov/node/54496; "Drone Operations," Government Accountability Office, https://www.gao.gov/drone-operations.

Key Concerns and Examples of Weaponization:

- *Potential for Malicious Use:* Drones can be easily outfitted with various weapons, including firearms, explosives, incendiary devices, or even chemical or biological agents, posing a risk to individuals, critical infrastructure, and government facilities.
    - *Terrorism:* terrorist organizations can adapt and exploit drone technology to target public spaces and infrastructure, potentially magnifying casualties and damage. Cartels operating in Mexico along the U.S. southern border are already using weaponized drones to drop munition payloads.
    - *Drone swarms:* Coordinated attacks utilizing drone swarms can overwhelm traditional defenses and enhance the effectiveness of sabotage operations.
- *Drone Incursions and Modern Espionage:* There have been numerous drone incursions over sensitive sites, including military bases and critical infrastructure, raising concerns about potential threats. Drones can be used for corporate and foreign espionage, including surveillance of facilities, intimidation through observation, and even cyberattacks by leveraging proximity to networks.
- *Smuggling and Criminal Activity:* Drones are used by criminals for illegal drug shipments, delivery of contraband into prisons, and counter-surveillance of law enforcement.
- *Privacy Concerns:* Drones equipped with cameras and other sensors can be used for unauthorized surveillance and invasion of privacy.
- *Interference with Public Events and Aircraft:* Unauthorized drone flights can disrupt public events and pose a risk to aviation safety, including the potential for collisions with manned aircraft.

Common commercial drones have already been used in attempts to destroy or damage critical infrastructure, and we continue to see variations of weaponized drones attempting to attack the public in the heartland and law enforcement in cities and on the border.

- *2020 Pennsylvania Power Substation Incident:* A modified drone was discovered outside an electrical substation in Pennsylvania. It was equipped with a copper wire, likely intended to create a short circuit and disrupt power. The drone crashed before reaching its target, but it highlights the potential threat.
- *Attempted Attack in Nashville (2024):* A man was arrested in November for planning to use a weapon of mass destruction to attack an energy facility in Nashville. Court documents indicated he planned to use a drone to deliver an explosive.
- *Suspicious Drone Activity near Energy Sites (2024):* In December, multiple energy sites requested temporary flight restrictions due to unusual drone activity in New Jersey, New York, and Maryland. Although the operators weren't identified, this incident reflects the ongoing concern about drone threats.

What is Our Current Airspace Protection Posture?

Over the years, drones have evolved from simple weekend toys to sophisticated tools used for smuggling, corporate espionage, and terrorist surveillance. Unfortunately, federal policies have struggled to keep up with these emerging threats, leaving state, local, tribal, and territorial (SLTT) law enforcement agencies in a challenging position and their constituents unprotected. These agencies and trained security professionals are on the frontlines protecting critical locations—such as stadiums, power plants, and city skylines—but they face legal restrictions that prevent them from effectively addressing drones that pose a danger to these sites and the American public.

As you know, only a few federal law enforcement components in the Department of Homeland Security (DHS), Justice (DOJ), and Defense (DoD)—have explicit legal authority under 6 U.S.C. § 124(n) and 10 U.S.C. § 130(i) to detect and mitigate (or stop) illicit drone activities. Other entities, including state and local police departments and trained security professionals, must rely on federal support or remain powerless, while unidentified drones fly dangerously over parades, concerts, major sporting events, and critical infrastructure. By their own admission, the DOJ and DHS can only respond to less than one percent of the thousands of counter-drone operational requests they receive each year.

According to FAA data and previous DoD testimony, drone incursions have steadily increased since the establishment of federal counter-drone authorities in 2018. First responders report that drones are tailing SWAT teams, dropping contraband into prisons, spying on neighbors, and hovering over chemical plants. While the threat is local, the legal tools remain predominantly federal in nature.

In 2014, while serving as the National Security Council Director for Aviation Security at the White House, we encountered drone incursions on the White House and Capitol campuses. Subsequently, the interagency met to develop a response plan for these "non-traditional aviation threats." As a result of these efforts, the FAA received Congressional direction to begin testing counter-drone technology systems in 2016. In 2017, the Department of Defense was granted additional authorities. In 2018, Congress authorized a five-year pilot program for federal law enforcement as part of the FAA Reauthorization process to provide counter-drone authorities to the Department of Homeland Security (DHS) and the Department of Justice (DOJ). Seven years later, these authorities remain unchanged.

DHS, DOJ, the security industry, and state, local, tribal, and territorial (SLTT) law enforcement agencies and trained security professionals have repeatedly urged Congress to expand authorities to enable air domain awareness and drone protection in American communities and over our critical infrastructure. Unfortunately, those requests have not resulted in any expanded or new authorities, and the limited authorities from 2018 have been periodically renewed only for short periods of time, creating uncertainty for law enforcement and the industry.

LEGISLATIVE RECOMMENDATIONS AND NEXT STEPS

The President's recent executive orders are a good start to address our legislative and regulatory inaction. However, executive action alone is not a permanent shield—it can be revoked by future administrations or challenged in court. Congress must move now to codify SLTT counter-UAS authorities with the same privacy safeguards and oversight as outlined in President Trump's executive orders.

I strongly urge the Subcommittee and full Committee to take bipartisan legislative action now. The industry, public safety professionals, and the American public are calling for three simple actions that can be taken immediately to make Americans and our skies safer.

1. Expand the current 6 U.S.C. §124(n) detection and mitigation authorities to all SLTT-LE and trained security professionals, safeguarding our critical infrastructure, and amend 49 U.S.C. § 14501 to include an explicit "Counter-UAS Exception," authorizing approved non-federal entities to employ safe and effective, non-kinetic mitigation under DHS oversight.
2. Develop, implement, and oversee a counter-drone operator training regime, using a federally accredited curriculum required for all counter-drone operators using approved mitigation

technology; and

3. Provide dedicated funding programs that enable critical infrastructure operators to procure, train, deploy, and operate counter-drone systems deemed safe and effective by the federal government.

CONCLUSION

The tactics developed in overseas drone conflicts—such as persistent surveillance, sabotage using payload delivery, loitering munitions, and swarm saturation strikes—are now poised to harm us at home. The increasing number of drone incursions into sensitive airspace we've seen in recent years should serve as a loud and distinct alarm bell, warning us of the immediate necessity for deploying safe and effective counter-drone technology to enable rapid response capabilities. While the industry has developed effective detection, identification, and mitigation solutions, challenges such as legal uncertainties, regulatory delays, and funding shortages are hindering nationwide implementation. To address these issues, Congress should clarify its legal authorities, streamline the approval process, and establish dedicated funding. This will enable U.S. stakeholders to effectively deter and counter drone-related threats before they reach our shores. Now is the time to strengthen our defenses in the skies before tomorrow's headlines report the first successful drone strike on U.S. soil.

Thank you for your leadership and the opportunity to appear before you today. I look forward to answering any questions you may have.

Figure 1
Drone Threat Progression Abroad and in the Homeland

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

STATEMENT OF

MR. PAUL CHURCHILL HUTTON IV

CHIEF GROWTH OFFICER, AEROVIRONMENT, INC. (AV)

8 JULY 2025

Chairman Gimenez, Ranking Member McIver, and Distinguished Members of the Subcommittee, thank you for the opportunity today to testify on how drone warfare abroad is transforming and informing domestic investments to prepare for threats here in the United States. I commend this committee's focus on these national security challenges along with your efforts to enhance the safety of U.S. transportation systems. The collaboration between Congress and industry is essential to keeping the American people and critical national infrastructure safe from today's rapidly evolving drone threats.

AV has a unique vantage point in this space as the top producer and supplier of Unmanned Aerial Systems (UAS) to the Department of Defense (DoD) coupled with our layered counter-UAS solutions deployed to multiple conflict zones abroad. This gives us a holistic view of the UAS threats, mitigation tools, and relevant implications for homeland security. The lessons we have learned from operations abroad underscore the urgent need to address this threat with greater speed and resolve to protect critical U.S. infrastructure and public safety including at high-visibility events like the 2026 FIFA World Cup, America's 250th birthday celebrations, and the 2028 Summer Olympics. In order to accomplish this goal, we believe it is vital that the U.S. Government and Industry have three key things in place: 1) a resolve to adopt lessons learned from real operational feedback; 2) flexible sources of funding to modify or scale up the production and delivery of new, software defined platforms that can be updated in response to evolving threats, and 3) the necessary authorities to allow federal and state government users to employ technology solutions in what we know are complex jurisdictional scenarios.

Threats and evolving environment

As a former soldier who benefited from DoD's nascent UAS arsenal over two decades ago, I commend this panel for bringing awareness to the American people regarding the proliferation of UAS technology - particularly how its capability, lethality, availability, and quantity, when combined, can enable malign actors to threaten unprotected infrastructure and lives.

Looking abroad, Ukraine's recent "Operation Spider's Web" against Russia's strategic bomber infrastructure demonstrated the precision, reach, and destructive ability of small UAS. Spider's Web highlighted the rapid evolution of small drone system capabilities at an affordable cost. The reports of covert Ukrainian launches from inside Russia emphasize the need for agile, real-time government and industry collaboration to develop detection systems and interdiction tools here at home. Municipal, state, and federal agencies need to adequately prepare for unmanned and increasingly autonomous systems in their public safety and security strategies.

More recently, in June 2025, during a 12-day conflict with Iran, Israel coordinated a drone and missile campaign targeting Iranian air defenses, ballistic missile platforms, and command infrastructure. While Israeli fighter jets visibly degraded Iran's missile sites and attacked military personnel, Israeli drones, pre-positioned quadcopters, and internet-connected launch platforms operated from within Iran, showcasing this new frontier of drone warfare.

The implications for the defense of our homeland is significant. The use of drones built from commercial parts and operated with minimal infrastructure is increasingly plausible by proxy networks or lone actors on domestic soil. Techniques like drone swarming, GPS jamming, and antiradar flights, perfected abroad, could be adapted to threaten critical U.S. infrastructure.

In the maritime environment, UAS pose a significant threat to shipping in vital trade chokepoints. From 2023 to 2024, there were over 50 UAS incidents in the Red Sea, many involving direct attacks or surveillance of commercial vessels. The increasing frequency and sophistication of these drone operations, by state and non-state actors alike, highlight the urgent need for improved countermeasures to protect critical maritime infrastructure.

Closer to home, unidentified aerial objects have reportedly entered U.S. airspace off the East Coast and have raised national security concerns. From 2021 to 2024, over 30 incidents were reported, with objects demonstrating advanced maneuverability and speed. These incursions underscore the critical need for advanced detection and mitigation technologies to protect key maritime regions and ensure U.S. airspace security.

Activities at the Southern Border continue to pose a direct threat to our homeland, as transnational criminal organizations, gangs, and extremist organizations adopt UAS to aid in their transport of illicit material into the U.S. The defense industrial base is poised to work with Congress and our executive branch counterparts to ensure we are prepared for UAS incursions and possible attacks through our own borders.

Many of your industry partners recognize these threats and are developing robust countermeasures today. Although these investments are taking place, many challenges remain–requiring Congressional, Federal Executive, plus State, local, and municipal action.

Challenges

Traditional defense acquisition processes are inadequate to deliver the capabilities necessary to outpace the fast-evolving UAS threat. We can no longer afford multi-year requirements development followed by lengthy science and technology experimentation

cycles. Government and industry must work together to develop and field new agile counter-UAS programs, and pair these programs with key authorities designed to protect critical infrastructure.

Effective solutions require affordable, open, and adaptable technologies rather than high-cost, proprietary systems. Operational clarity and streamlined authorities are essential for establishing guidelines for UAS detection and defeat within domestic airspace. Government and industry partnership will benefit all parties, maximizing innovative and delivering cost-effective solutions.

Solutions must be tailored to meet the unique demands of countering UAS threats. To succeed, we need acquisition reform—but we also need operational clarity. Homeland security stakeholders must work together to establish operational directives that define authorities for UAS detection, identification, and defeat in domestic airspace and enable responsible action under clearly defined legal and safety parameters.

The rapid increase in UAS lethality—as demonstrated in the Ukraine conflict, where drones now cause the majority of casualties—serves as a stark warning. Our traditional defenses and authorities have not kept pace, and we must act swiftly to prevent similar threats against our infrastructure and population.

Opportunities

U.S.-based defense innovators are developing promising systems to detect, track, and defeat UAS threats. Soft-kill techniques, such as jamming or radio frequency (RF) manipulation, have dominated this space in the past five years. In an effort to combat these defensive tactics, adversaries increasingly employ drones guided by fiber optics, preprogrammed autonomy, various frequency bands, or cellular signals. A few systems, like ours at AV, have capabilities against GPS. The existing authorities make it difficult to utilize these advanced technologies, so we are expanding our ability to counter peer threat capable systems. In parallel, we must continue the development of hard-kill solutions—systems that physically destroy or disable drones.

As has been heard in testimony before other House committees, the President's budget requests critically needed investments in drone technologies and policy changes to improve acquisition and production of drone systems, at scale. The government is poised to be able to take advantage of fast-moving private sector innovation to field low-cost, attritable, kinetic and non-kinetic UAS and counter-UAS systems.

Detection technologies, directed energy (laser) and kinetic defeat capabilities offer a promising path forward. The U.S. Army, for example, has demonstrated the effectiveness of high energy laser systems deliver hard-kill effects with minimal collateral damage. When combined with acoustic sensors, passive radar, and software-defined radio receivers, this creates an integrated drone shield that can be safely deployed in mixed civilian environments focused today on small and medium-sized UAS at close range. Kinetic alternatives, like the Army's Next Generation Counter-UAS Missile, complement directed energy solutions, allowing affordable defense at greater range, elevation, and weather scenarios, though the employment of these systems would be limited in accordance with the sensitivity of the protected infrastructure and public safety requirements. Kinetic solutions are more effective against large UAS, which have been used extensively in Ukraine and the Middle East. These offerings provide alternatives to the unsustainable practice currently employed of shooting down low-cost drones with multi-million-dollar weapons systems, which are expended upon use and difficult to replace.

These technologies are ready, but they require strong demand signals, enabling policies, and streamlined authorities to mature and scale. Without decisive action, the U.S. risks trailing our adversaries' rapid innovations. We need expanded authorities for UAS defeat operations inside US borders, clear operational doctrines, and funding structures that reward responsiveness. With additional authorities and funding, the defense industrial base can meet the needs of the country. Affordable, attritable platforms at mass are transforming the way in which we fight and are rapidly evolving in a way that necessitates we take advantage of solutions available today, both custom and commercial. We commend the DoD's continued efforts to eliminate overly bureaucratic processes and fund the fielding of systems across all domains.

AV, alongside other forward-leaning, innovative U.S. companies, stands ready to meet this challenge. However, policy inertia and acquisition drag–not technology–remain our most significant obstacles. It is encouraging to see agencies like DoD, DHS, and members of Congress and committees like yours begin to take steps to rectify the issues we face today. All parties understand that we must act now to prevent foreign battlefield experiences from becoming domestic tragedies.

Thank you again for the opportunity to testify. I look forward to your questions.

TESTIMONY OF

Michael Robbins
President & Chief Executive Officer
Association for Uncrewed Vehicle Systems International (AUVSI)

BEFORE

U.S. House of Representatives
Committee on Homeland Security
Subcommittee on Transportation and Maritime Security

Surveillance, Sabotage, and Strikes: Industry Perspectives on How Drone Warfare Abroad Is Transforming Threats at Home

ON

July 8, 2025
Washington, DC

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

Thank you for the opportunity to testify before you today. My name is Michael Robbins, and I am the President and CEO of the Association for Uncrewed Vehicle Systems International (AUVSI), the world's largest nonprofit trade association dedicated to the advancement of uncrewed systems, autonomy, and robotics. AUVSI represents a broad spectrum of stakeholders who are committed to the secure, responsible, and innovative integration of drones and other autonomous technologies into our national airspace system and associated infrastructure.

The topic of this hearing could not be timelier. Across the globe, including ongoing conflicts in Ukraine, Africa, and the Middle East, we are witnessing a transformation in modern warfare and at the center of this transformation are uncrewed systems, in particular, unmanned aircraft systems (UAS or drones). Drones transform battlefields because they both extend operational reach as well as reduce the risk to human life. As I have said on a number of occasions, including in recent Congressional testimony, robots don't bleed.[1]

But this hearing is not just about foreign battlefields. What happens abroad is actively shaping the threat landscape here in the United States. Unfortunately, to date, what is happening abroad has not yet meaningfully changed our policy landscape to mitigate these threats. Inexpensive, consumer and commercial drones that are easily accessible and widely available are being modified to carry out surveillance, cyber disruption, espionage, and kinetic attacks against critical infrastructure. State sponsored and criminal actors are increasingly looking to these platforms for asymmetric advantages because they are accessible, inexpensive, adaptable, and often undetectable by legacy air defenses. Drone warfare abroad has shown us what's possible, and just as significantly, what's vulnerable.

As the title of today's hearing suggests, the same systems transforming how we move goods, inspect infrastructure, and save lives through public safety operations are also reshaping the threat landscape. Drones are inherently dual-use. Their commercial potential is vast and offers tremendous promise, yet their accessibility and adaptability also make them attractive tools for malicious actors. It is imperative that federal policy both leverages the benefits of these technologies and mitigates the emerging risks. Innovation and security must advance in lockstep.

U.S. airports, maritime facilities, power plants, prisons, amusement parks, sports stadiums, and even statehouses have increasingly seen incursions by unauthorized drones. While most are not overt attacks, they are proof points of how porous our defenses remain. Unfortunately, despite the many responsible drone users and operators around our country, especially those operating under Federal Aviation Administration (FAA) rules including Part 107 and Part 135, there are rogue actors looking to utilize these critical life-saving tools for nefarious purposes.

Yet our domestic policy and regulatory framework has not kept pace with the threat. There is no singular federal authority to counter uncrewed threats, no consistent framework for what technologies can be deployed or by whom, and no mandated reporting of drone incidents that could inform a national picture of risk. Congress has not updated our nation's UAS detection and

[1] AUVSI Testifies Before House Aviation Subcommittee on FAA Reauthorization Implementation with Emphasis on Drone & Advanced Air Mobility Regulations - AUVSI

mitigation authorities since 2018.[2] Meanwhile, the airspace has evolved tremendously, the threat landscape has changed dramatically, and the number of drones operating in the U.S. has expanded exponentially.

The lack of federal action and investment has left a dangerous gap in our ability to respond to reckless or nefarious drone activity. Today, only four federal agencies, the Department of Defense (DoD), Department of Homeland Security (DHS), Department of Energy (DOE), and Department of Justice (DOJ), are authorized to detect and mitigate UAS threats, and their authorities are very limited. State and local law enforcement, airport and prison operators, and other critical infrastructure entities are left watching and waiting while unauthorized drones fly overhead.

Today, only a limited number of top tier events are able to get federal support and equipment painting a clear picture of the airspace. If something catastrophic happens – a drone collision with a passenger aircraft, an attack on a packed stadium, or an intrusion into a sensitive government facility – finger-pointing will be inevitable. Congress, the White House, FAA, DHS, industry, and local authorities will all scramble to assign blame. But pointing fingers won't prevent a crisis, acting now will.

AUVSI applauds the Trump Administration's recent executive orders, *Restoring American Airspace Sovereignty*[3] and *Unleashing American Drone Dominance*[4], that addressed some counter-UAS (c-UAS) related issues and showcased the importance this Administration places on drone issues, but Congressional action is still necessary to expand c-UAS authorities.

The threats we're examining today demand a serious and coordinated response, one that strengthens our ability to defend against malicious use of drones while also preserving the critical benefits these technologies bring. Every day, drones support law enforcement, firefighters, energy providers, and emergency response teams in protecting lives and infrastructure. As we enhance our national security posture, it's essential that we also sustain the innovation and trusted uses that serve our communities. Striking that balance is not only possible, but also essential to both our security and our continued progress.

The Dual-Use Nature of Drones: A Strategic Asset and a Tactical Threat

Events unfolding around the world are not just instructive, they are sounding an alarm we cannot afford to ignore.

In Ukraine, the defense ministry's *Operation Spiderweb*[5] clearly showcased how swarms of small drones can be used to saturate enemy airspace, overwhelm air defense systems, and execute lethal strikes. These low-cost, high-impact platforms are changing the dynamics of warfare, not with brute force, but with agility, coordination, and volume. In the Middle East, Israel has leveraged drones to preemptively disrupt Iranian air defense networks, enhancing the safety and effectiveness of manned and unmanned aerial operations.

[2] https://www.auvsi.org/progress-on-domestic-uas-detection-mitigation-is-required-for-public-trust-enabling-drone-regulations/
[3] https://www.whitehouse.gov/presidential-actions/2025/06/restoring-american-airspace-sovereignty/
[4] https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/
[5] https://en.wikipedia.org/wiki/Operation_Spiderweb

These examples demonstrate a common truth: even small, commercially available drones, when used in a strategic and coordinated manner, can pose serious threats to fixed infrastructure. Ports, bridges, shipping terminals, and maritime chokepoints are all vulnerable to surveillance, sabotage, or disruption by hostile UAS activity. These vulnerabilities do not only exist in active war zones. They exist today, here at home, across the transportation and maritime sectors that support our national economy and security.

In short, the tactics we are witnessing in modern conflict zones are not constrained by geography. The barriers to entry are low, the technology is widely available, and the intent of our adversaries is clear. We must assume that the threat is already here, and we must act accordingly to protect the systems and infrastructure that keep this country not only moving, but safe.

Drones in Transportation and Maritime Security: A Critical Force Multiplier

Those very same drone systems that can be misused are also being used daily to protect American lives, infrastructure, and supply chains. Across the United States, transportation and maritime authorities are leveraging drones as essential tools for homeland security operations, providing perimeter monitoring, real-time subject tracking, and as part of Drone as First Responder (DFR) public safety programs. These applications allow rapid situational awareness and response to developing threats or incidents.

When used by trusted operators, with secure platforms, drones offer unmatched speed, agility, and visibility. They enable rapid situational awareness, improve officer safety, and shorten response times during high-risk incidents from port intrusions to natural disasters.

In infrastructure management, drones enable safe and cost-effective inspections of bridges, railways, pipelines, ports, runways, and more, tasks that would otherwise require human workers to operate in high-risk, unsafe environments. They provide real-time imaging and data that supports predictive maintenance and operational readiness. A particularly powerful example of the utility of drones came in the aftermath of the Francis Scott Key Bridge collapse in Baltimore, Maryland. Drones were immediately deployed by local and federal authorities to assist with damage assessment, guide search and rescue teams, and coordinate the emergency response. These operations illustrated the agility, speed, and value of drone systems in supporting critical transportation and maritime missions.

This is the dual-use reality we face. While malicious actors may seek to weaponize this technology, the overwhelming majority of use cases, particularly in public safety and critical infrastructure, are enhancing our ability to respond to threats and protect American lives. As policymakers, it is vital to distinguish between threats and trusted uses, and to ensure that our response to one does not hinder our ability to leverage the other.

National Security Risks from People's Republic of China (PRC)-Manufactured Drones

While drones are proving to be essential tools for homeland defense and emergency response, not all systems are created equal, and some represent an active and growing risk. Drones manufactured by companies with ties to the PRC continue to be widely used by public safety and other agencies, even in sensitive infrastructure environments. In some cases, federal agencies are still using these platforms. This is largely due to the absence of consistent federal procurement restrictions or

guidance and minimal oversight of mandates already enacted into law as part of the American Security Drone Act and other legislation.

The national security implications are stark and well documented. Numerous assessments by DoD, DHS, and other federal intelligence agencies have documented how PRC-made drones present unacceptable risks, including unauthorized data collection and transmission to the PRC.

AUVSI has been the tip of the spear in urging the swift implementation of Section 1709 of the Fiscal Year 2025 National Defense Authorization Act (NDAA), which would add the communications equipment and services of PRC drone manufacturers DJI and Autel Robotics (and any of their subsidiaries, affiliates, partners, joint venture entities, or entities with a technology sharing or licensing agreement with a named entity) to the Federal Communications Commission's (FCC) Covered List. This will occur after a relevant national security agency makes a determination on their unacceptable risk to national security, or, on 23 December 2025 as directed by Congress if action is not taken sooner.[6]

Despite these legitimate and documented concerns, many agencies continue to procure and operate PRC platforms due to a lack of consistent federal policy, market incentives, and clear alternatives. Allowing adversary-linked systems to operate in the heart of our national infrastructure networks is a liability we cannot afford. To defend against emerging threats, we must ensure that the platforms used to secure our infrastructure are not themselves potential vectors for surveillance, sabotage, cyber intrusion, or supply chain warfare.

This is not about cutting off access to drones, it is about ensuring that the platforms used to secure the homeland are not themselves Trojan horses. Allowing systems tied to adversarial governments to operate within our most critical infrastructure networks is a legitimate threat that we can address through commonsense action.

We cannot effectively defend against surveillance or sabotage if we continue to operate systems that may be compromised from within. Building a trusted, resilient domestic drone ecosystem is not just a competitive advantage, it's a national security necessity here in the United States.

Congress must act to accelerate the transition to trusted U.S. and allied systems, by setting clear procurement standards, supporting domestic manufacturing, and incentivizing the adoption of secure platforms.[7]

Advancing Security Solutions and Maritime-Specific Applications

Several mature, scalable solutions are already available and in use. Technologies such as Remote Identification (Remote ID), drone detection and tracking systems, and defensive mitigation tools, both kinetic and non-kinetic, have advanced significantly in recent years alone. These tools allow security personnel to identify, assess, and, when authorized, neutralize malicious drone activity.
While much of the public conversation has focused on protecting airports, stadiums, and federal buildings, our maritime and transportation infrastructure remains significantly under protected.[8]

[6] Whitepaper: AUVSI Partnership for Drone Competitiveness
[7] AUVSI - Rethinking Acquisition to Unleash American Leadership in Uncrewed Systems
[8] AUVSI Testifies at Congressional Hearing on the State of America's Maritime Infrastructure

Shipyards, ports, offshore energy platforms, rail crossings, and inland waterways are just as vulnerable to surveillance, sabotage, and disruption; and in many cases, even more difficult to secure due to their geographic scale and open access.

Adaptation of these technologies for maritime domains, including ports, shipyards, and offshore energy infrastructure, is both necessary and feasible. These critical nodes in our logistics and energy networks deserve the same layered protections that are being discussed for airports, stadiums, and government facilities.

Importantly, these efforts must be guided by clear federal frameworks that balance security with privacy, protect authorized drone operations, and enable public-private coordination. AUVSI urges Congress to support the deployment of scalable c-UAS solutions, particularly in cooperation with the U.S. Coast Guard (USCG), Customs and Border Protection (CBP), and the Department of Transportation (DOT). These agencies must be empowered and resourced to defend our maritime and other infrastructure effectively.

The Need for Expanded c-UAS Authorities and Thoughtful Regulation

Today, the federal government's ability to detect and mitigate rogue drones remains limited to a small number of agencies under narrow statutory authorities. This patchwork is unsustainable in the face of a growing and evolving threat.

I had the privilege of co-chairing the FAA's Section 383 UAS Detection and Mitigation Systems Aviation Rulemaking Committee, which brought together industry, government, and civil society to assess the legal and operational challenges of c-UAS deployments. One resounding conclusion: more entities need clearly defined, narrowly tailored authorities to engage in drone detection and mitigation activities, especially those protecting high-risk infrastructure.

We urge Congress to act on the Committee's recommendations, create a legal framework for authorized detection and mitigation operations, and ensure interagency coordination, privacy protections, and operator transparency.[9]

Congress should pass the bipartisan Disabling Enemy Flight Entry and Neutralizing Suspect Equipment (DEFENSE) Act which aims to protect outdoor sporting events from unauthorized drones and enhances security at major outdoor gatherings and sporting events by ensuring that state and local law enforcement have the authority and tools necessary to protect these events from aerial threats in real-time, rather than waiting for federal intervention. The bill would give state and local law enforcement the authority to mitigate threats posed by drones in places where a temporary flight restriction is in place. This includes large outdoor and sporting events. It would also require DOJ, FAA, FCC, and the National Telecommunications and Information Administration (NTIA) to create a list of approved technology that local and state law enforcement officers can use to address these threats.

Additionally, it is imperative that Congress consider broad c-UAS legislation this Congress. Whether it is a refreshed version of the Counter-UAS Authority Security, Safety, and

[9] UAS Detection and Mitigation Systems Aviation Rulemaking Committee Final Report. January 9, 2024.

Reauthorization Act from the 118th Congress[10], which this Committee worked diligently on, or a something akin to the Safeguarding the Homeland from the Threats Posed by Unmanned Aircraft Systems Act[11], our country and threat landscape needs three critical things – modernization, protection, and progress.

Conclusion and Recommendations

Drone technology is transforming the landscape of transportation and maritime security, creating both unprecedented capabilities and new avenues of risk. As we've seen on the global stage, drones can be tools of war, espionage, and disruption. But they are also indispensable assets in defending the homeland, securing our infrastructure, and responding to emergencies with speed and precision.

As the threats are evolving rapidly, so must our policies, capabilities, and posture. The time for federal leadership is now.

To meet this call to action, AUVSI recommends that Congress take the following actions:

1. Expand c-UAS authorities to additional federal agencies and delegate detection authorities to state, local, tribal, and territorial (SLTT) agencies operating at critical sites, with appropriate and robust federal training and oversight, and delegate mitigation authorities in more limited instances, again with significant federal training and oversight.
2. Enact legislation restricting PRC-manufactured drones from use in critical infrastructure environments, inclusive of a suitable transition period, and a funding stream that provides support for operators to transition their fleets away from unsecure PRC platforms to secure domestic or allied alternatives.[12]
3. Support domestic drone production and adoption of secure, trusted systems through advanced market commitments, grant programs, tax incentives, loan guarantees, and other federal mechanisms.
4. Invest in detection, Remote ID, and mitigation technologies, including maritime applications.
5. Promote interagency coordination through unified national strategies and continued stakeholder engagement.

Thank you again for the opportunity to testify today, as well as the Committee's leadership and focus on these urgent issues. AUVSI and its members stand ready to support this Committee and the broader Congress in advancing smart, secure, and future-ready drone policies that defend our homeland while enabling innovation and trusted use.

I look forward to your questions.

[10] https://www.congress.gov/bill/118th-congress/house-bill/8610/text/
[11] https://www.congress.gov/bill/118th-congress/house-bill/4333/text
[12] Whitepaper: AUVSI Partnership for Drone Competitiveness