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