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

BEFORE

U.S. House of Representatives
Committee on the Judiciary
Subcommittee on Crime and Federal Government Surveillance

HEARING ENTITLED

Unmanned and Unchecked: Confronting the Rising Threat of Malicious Drone Use in America

ON

September 16, 2025
Washington, DC

INTRODUCTION

Chairman Biggs, Ranking Member McBath, and distinguished members of the Subcommittee, thank you for the honor of appearing before you today. I commend this Subcommittee for its proactive focus on a threat that has rapidly evolved from a distant concern into a clear and present danger to our national security, critical infrastructure, and public safety.

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, a group comprised of the leading providers of C-UAS technologies available around the world, as well as the security service providers and integrators that use these products to carry out critical public safety functions. Throughout my time in law enforcement, the military, and as a federal civilian, I was dedicated to the safety and security of our great nation. Now in the private sector, the mission is no different, and I am honored to appear before the Subcommittee representing both D-Fend Solutions and the drone security industry.

I am here today to discuss the rising and multifaceted threat posed by the malicious use of unmanned aircraft systems (UAS), or drones. The accessibility, affordability, and adaptability of this technology have democratized aerial capabilities. Still, in doing so, they have also created a significant vulnerability that we, as a nation, are not yet prepared to fully address.

THE EVOLVING THREAT LANDSCAPE

The malicious and illicit use of drones has evolved beyond simple nuisance to become a realm of organized, sophisticated threats and criminal activity. We can categorize this threat into three primary domains:

1. Criminal and Illicit Activities:

The use of drones by transnational criminal organizations, terrorist organizations, including cartels, domestic gangs, and individual bad actors, is no longer hypothetical. Incidents of drones being weaponized or used to deliver contraband—from drugs and weapons to cell phones—into correctional facilities are a daily occurrence. The challenge is not only at the federal level, but at state and local correctional facilities as well, all of which are often ill-equipped to detect or counter these incursions. The ability of drones to bypass traditional security perimeters makes them a favored tool for illicit trade.

2. Physical and Cyber-Attacks on Critical Infrastructure:

The potential use of drones in attacks on critical infrastructure is alarming. A drone with a small payload could significantly damage power substations, water treatment plants, or communication towers, causing widespread disruption and economic turmoil. Unauthorized incursions over sensitive sites, such as military bases and recent drone sightings in New Jersey, highlight this threat. The emergence of AI-enabled, autonomous drones adds another layer of complexity to the detection and response ecosystem.

3. Surveillance and Espionage:

Drones offer a low-cost, low-risk platform for persistent surveillance. They can be equipped with sophisticated cameras, thermal sensors, and even Wi-Fi sniffing technology to gather intelligence from

a distance, without the need for physical access. This capability is particularly concerning when considering foreign adversaries and their state-sponsored actors. The widespread use of commercially available drones manufactured by foreign entities raises significant counterintelligence risks, as data collected by these devices could be exfiltrated back to hostile governments.

CHALLENGES IN CONFRONTING THE THREAT

Despite the clear and growing danger, our current legal and technological frameworks have not kept pace. Key challenges include:

Fragmented Authorities: The authority to detect and mitigate malicious drones is fragmented across various federal agencies, including the Department of Homeland Security, the Department of Justice, the Department of Defense, and the Department of Energy. This lack of a single, unified authority across the Federal government creates confusion and potential gaps in response, especially for state and local law enforcement and trained security professionals protecting critical infrastructure.

Technological and Legal Gaps: While safe and effective Counter-UAS (C-UAS) technology exists, such as RF-Cyber takeover systems, its use is severely restricted by the interpretation of existing laws formed well before drone technology became prominent. Law enforcement has the legal authority to pursue and stop a suspicious car operating illegally, but still lacks the legal standing or authority to use technology to do the same with a drone in a safe and timely manner.

Lack of Uniformity: The FAA has made strides in regulating drone operations, but a patchwork of state and local laws has created an inconsistent legal landscape. This makes it difficult for law enforcement to act decisively and for responsible drone operators to understand and comply with regulations. It also leaves law enforcement and the public wondering what is legally or illegally flying above their communities. I cannot overstate the immediate need for clear, expanded detection, tracking, and identification authorities enough to ensure our communities have complete air-domain awareness of drone activity across America.

RECOMMENDATIONS

To address these challenges, I respectfully offer the following recommendations for the Subcommittee's consideration:

1. Comprehensive Federal C-UAS Legislation: Congress must pass legislation that provides a clear and cohesive framework for C-UAS operations across the United States. This legislation should:

- **Expand Existing C-UAS Authorities:** Clarify and expand the legal authority for all federal agencies, state, local, tribal, and territorial law enforcement, and trained security professionals protecting our critical infrastructure to use C-UAS technologies to detect, track, and identify drone threats.
- **Expand the Existing Pilot Program**: Expand the 2018 Federal Pilot Program for mitigation of drone threats to include all federal agencies, state, local, tribal, and territorial law enforcement, and trained security professionals. The original 5-year pilot program is now in its eighth year. It needs to be expanded in a manner and scale commensurate with the rapid emergence of new technologies and the growing threat to our society from the illicit use of drones. Failure to do this creates significant risk to our ability to safely and securely host the World Cup, America's

250th anniversary celebrations, hold elections, and host the 2028 Olympics.

2. Inter-Agency Collaboration and Information Sharing: An ability for law enforcement to review the FAA's drone registry information through the existing National Crime Information Center (NCIC), like we do with vehicle registration and license plates, would better enable law enforcement to protect the public in a safe and efficient manner that is consistent with current privacy and civil liberty laws.

3. Public Awareness and Education: Like operating a car, you can either fly drones legally or illegally, and after years of FAA awareness campaigns, ignorance of the law is no longer a defense for recklessly flying in our nation's airspace. We must launch a robust public awareness campaign to educate citizens on the dangers and illegality of careless and malicious drone use. This campaign should emphasize the potential for severe legal penalties for unauthorized drone operation in restricted areas.

CONCLUSION

In conclusion, the threat from malicious drone use is real, immediate, and growing. We have seen what these platforms are capable of in conflicts abroad, and we are already seeing these same tactics being adapted for use against our communities and our country.

By taking decisive action now to modernize our laws, enhance our technological capabilities, and strengthen the partnerships between all levels of government, we can ensure that our skies and citizens on the ground remain safe and that the promise of unmanned technology is never subverted by those who seek to do us harm.

Thank you, and I look forward to your questions.

Respectfully Submitted,

BRETT J. FEDDERSEN
Vice President of Strategy and Government Affairs at D-Fend Solutions AD, INC
Chair of the Security Industry Association's Drone Security Subcommittee