

Critical Issues in Policing

A Clear and Present Danger

The Rise of Malicious Drones
and What Police Executives Can Do About It



2026



Critical Issues in Policing

A Clear and Present Danger

The Rise of Malicious Drones
and What Police Executives Can Do About It

September 2026



Recommended citation:

PERF (Police Executive Research Forum). 2026. *A Clear and Present Danger: The Rise of Malicious Drones and What Police Executives Can Do About It*. Critical Issues in Policing Series. Washington, DC: Police Executive Research Forum.

This publication was supported by the Motorola Solutions Foundation. The points of view expressed herein are the authors' and do not necessarily represent the opinions of the Motorola Solutions Foundation or all Police Executive Research Forum members.

Police Executive Research Forum, Washington, D.C. 20036

Copyright © 2026 by Police Executive Research Forum

All rights reserved.

Printed in the United States of America.

ISBN: 978-1-934485-86-6

All photos by Dustin Waters except where otherwise indicated.
Graphic design by Melissa Fox and Dustin Waters.

Contents



A Message from Executive Director Chuck Wexler.....	v
Acknowledgments	ix
Executive Summary.....	xi
Introduction	1
Drone Technology—Seven Years of Change	5
Early Warnings About Drone Threats	5
Why Has Local Law Enforcement Historically Lacked C-UAS Authority?	8
As Drones Became More Capable, Concerns Intensified.....	10
The Growing Risk of Malicious Drone Operations.....	15
Concerns about Foreign-Made Drones	18
Increasing International Use of Drones for Criminal Activity	18
The Increasing Domestic Use of Drones for Criminal Activity	21
International Events Hosted in the United States	22
Recent Changes to Resources and Authority.....	27
Executive Orders	27
The SAFER SKIES Act	30

Eight Things Agencies Can Do Before NCUTC Certification 33

- 1. Build Public Support for Counter-UAS Operations 34
- 2. Establish Relationships with the Key Counter-UAS Specific Federal Agencies 34
- 3. Determine Where the C-UAS Function Will Reside 35
- 4. Plan Ahead for Special Events 35
- 5. Assess Critical Infrastructure 37
- 6. Develop and Implement Lawful Detection Capabilities 38
- 7. Report Every Significant Drone Incident. 41
- 8. Pursue NCUTC Training and Agency Accreditation. 41

After Certification—Four Ways to Build a Sustainable C-UAS Capability 43

- 1. Move Toward Independent Operations 43
- 2. Develop Internal Policy and Oversight 44
- 3. Integrate C-UAS into Existing Operations 45
- 4. Build Sustained Proficiency 45

Conclusion 47
Appendix A. Glossary 49
Appendix B. Resources 51
 The Police Executive Research Forum..... 55
 The Motorola Solutions Foundation 57

A Message from Executive Director Chuck Wexler



Twenty-five years ago on 9/11, our country suffered a terrorist attack that resulted in an unthinkable loss of life and injuries on a massive scale. In the wake of that tragedy, the 9/11 Commission concluded that the attacks revealed four types of failures across government: “imagination, policy, capabilities, and management.”¹ It is no mistake that the failure of imagination is listed first; simply stated, too few people were willing to imagine how existing technologies could be used in new ways to cause massive and devastating harm.²

We may be facing a similar failure of imagination today, this time involving the malicious use of drones.

Seven years ago, PERF released its first report on drone use by law enforcement: *Drones: A Report on the Use of Drones by Public Safety Agencies—And a Wake-up Call about the Threat of Malicious Drone Attacks*.³ As the title suggests, the report examined not only the benefits of drone technology for public safety agencies but also the emerging threat posed by malicious drone use.

Much has changed since that report was published. Russia’s 2022 invasion of Ukraine transformed the modern battlefield and demonstrated the rapidly evolving role of drones in military operations and attacks against civilian infrastructure. Since that invasion, I have traveled to Ukraine four times, most recently in October 2025. On that visit, I traveled with a cross-section of law enforcement leaders, including philanthropist and former Macon County (Illinois) Sheriff Howard Buffett, who has made support for Ukraine a top priority for his foundation and has traveled to the war-torn nation many times; we saw firsthand how the drone threat has evolved. Drones that in the past

-
1. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: U.S. Government Printing Office, 2004), 339, <https://www.govinfo.gov/app/details/GPO-911REPORT>.
 2. National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (see note 1).
 3. PERF (Police Executive Research Forum), *Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks* (Washington, DC: Office of Community Oriented Policing Services, 2020), <https://www.policeforum.org/assets/Drones.pdf>.

relied on radio frequencies or GPS signals, which could often be disrupted through jamming, are increasingly impervious to traditional countermeasures. Some are guided by artificial intelligence, allowing them to operate with little or no active signal to intercept. Others are connected to their operators through fiber-optic cables that can stretch for miles, eliminating the radio transmissions many counter-drone systems are designed to detect or disrupt.

What struck me in Ukraine was the extent to which drones have come to dominate the war on both sides—drones are everywhere. They gather intelligence; drop explosives; resupply front-line troops with food, water, and medical supplies; and pose a pervasive and constant threat. After that visit, I wrote a column warning that “we are likely to see an attack involving drones in the near future, and local police are not currently in a good position to counter the threat.”⁴

But since that warning, things have begun to change. In 2025, Congress passed the SAFER SKIES Act, creating, for the first time, a pathway for state and local agencies to obtain real counter-UAS authority—the ability not just to detect a malicious drone but also to take action against it. That legislation included \$500 million in grant funding for training and equipment and helped spur the creation of the FBI’s National Counter-UAS Training Center in Huntsville, Alabama, which now trains officers from around the country. Coupled with two 2025 Executive Orders directing agencies to formalize local counter-drone capabilities, these developments represent the most significant expansion of local counter-drone capability in American history.



4. Chuck Wexler, “What American Can Learn from Ukraine about the Danger Posed by Drones,” *PERF Trending*, last modified November 1, 2025, <https://www.policeforum.org/trending1nov25>.

That progress was tested this summer. Local and federal authorities seized more than 700 drones operating near FIFA World Cup stadiums and fan festivals across 11 U.S. host cities. The tournament—like the America250 celebrations that followed it—concluded without a catastrophic incident. That is a credit to the planning, training, and interagency coordination that went into securing both events. But we should not mistake the absence of an attack for the absence of a threat. Seven hundred drone incursions in a matter of weeks is not evidence that the danger has passed—it is evidence of exactly how persistent and commonplace unauthorized drone activity has become, even around some of the most heavily secured airspaces in the country. The agencies that succeeded this summer did so not because they were lucky but because they had invested years in planning, training, equipment, and partnerships before any threats materialized.

New authority is arriving, but authority alone will not protect a stadium, a power plant, a public gathering, or critical infrastructure. Counter-drone capability must become a core component of public safety preparedness, not a specialized function reserved for major events or large agencies. The same lesson that emerged from Ukraine, and later from the World Cup and America250 celebrations, is clear: Preparation matters. Agencies that build the necessary policies, partnerships, training, and technical capabilities now will be far better positioned to confront tomorrow's threats.

The lessons of the 9/11 Commission remain relevant today. The greatest danger is not simply that malicious drones exist. It is that we see the warning signs, understand the technology, and still fail to imagine what could happen next with this clear and present danger. Twenty-five years ago, our nation paid a terrible price for a failure of imagination. We cannot afford to make the same mistake again. This report is intended to help law enforcement leaders anticipate the threat, prepare for it, and act before a preventable tragedy becomes another national lesson.

Best,

A handwritten signature in black ink that reads "Chuck Wexler". The signature is fluid and cursive, with a long horizontal stroke at the end.

Chuck Wexler
Executive Director
Police Executive Research Forum
Washington, DC



Photo courtesy Lowell (Massachusetts) Police Department



Acknowledgments

This is the 57th report in PERF's Critical Issues in Policing series, a long-running project made possible by the generous and committed support of Motorola Solutions and the Motorola Solutions Foundation. PERF would like to thank Greg Brown, Motorola Solutions Chairman and CEO; Jack Molloy, Executive Vice President and Chief Operating Officer; Jason Winkler, Executive Vice President and Chief Financial Officer; John Zidar, Senior Vice President, North America Government; and Wesley Barden Touhy, Executive Director, Motorola Solutions Foundation.

Every PERF publication is the result of tremendous effort by many people, and this report was no exception. Center for Management and Technical Assistance Deputy Director Jennifer Sommers oversaw the production of this report, working alongside former *Washington Post* reporter Tom Jackman on the writing and editing. Senior Principal Dave McClure developed and managed the project, including conducting background research, designing the questionnaire, convening participants, and outlining this report. Senior Research Assistant Rachael Thompson assisted with meeting preparations and logistics. Director Tom Wilson provided leadership and guidance throughout the project. Communications Associate Dustin Waters supported the meeting through visual design; he also contributed to the report's layout, photography, and overall design. Melissa Fox, PERF Editor, edited the report with assistance from Communications Principal James McGinty.

The Federal Bureau of Investigation (FBI) provided key personnel whose expertise and contributions were invaluable to the development of this report. PERF is especially grateful to FBI leadership for authorizing the Bureau's participation in this effort and extends its appreciation to Assistant Director Leo Schmitz, Unmanned Aviation Section Assistant Section Chief Micheal Torphy, and members of the National Joint Terrorism Task Force for their attendance and active participation in the May 7, 2026, meeting. This publication would not have been possible without their insights, expertise, and support.

PERF also wishes to acknowledge Serhii Bolvinov, Deputy Chief of the Kyiv Regional Police in Ukraine, for traveling to the United States to brief law enforcement officials on how malicious drones are affecting the war against Russia and the lives of Ukrainian citizens. We are grateful for his participation.



Photo courtesy Arlington (Texas) Police Department



Executive Summary

The threat posed by malicious drone (unmanned aircraft system [UAS]) activity has grown from a hypothetical concern to an operational reality. In 2025 alone, the National Football League (NFL) reported 2,800 drone incursions into its stadiums, the New York City Police Department (NYPD) logged roughly 23,000 illicit drone flights per month, and the Federal Bureau of Investigation (FBI) seized more than 700 drones near World Cup venues across 11 host cities.⁵ Even so, local law enforcement lacked the independent legal authority necessary to address these threats as they emerged. As one official put it, even the most advanced local detection system remains “woefully inadequate” without the authority to act on a threat once it has been identified.

This gap between the ability to detect a threat and the authority to respond to it is not new. PERF first warned of it in 2019,⁶ but in the seven years since, UAS technology has evolved more rapidly than the laws governing it.

Malicious drone use has escalated internationally. UAS tactics have evolved on both sides in Russia’s war with Ukraine (see sidebar on page 16–17). Mexican cartels are weaponizing agricultural drones.⁷ And the 2026 conflict involving Iran, Israel, and the United States has seen thousands of drones launched toward the United Arab Emirates (UAE), with some striking areas near a nuclear

5. FAA (Federal Aviation Administration), “Successful Counter-Drone Efforts Helped Keep Millions of Fans Safe During FIFA World Cup 2026, With More Than 700 Drones Seized,” *FAA Newsroom*, July 22, 2026, <https://www.faa.gov/newsroom/successful-counter-drone-efforts-helped-keep-millions-fans-safe-during-fifa-world-cup-2026>.

6. PERF, *Drones: A Report on the Use of Drones by Public Safety Agencies* (see note 1).

7. Vanda Felbab-Brown, “How Mexican Cartels are Using Drones, Now and in the Future,” Brookings, last modified February 18, 2026, <https://www.brookings.edu/articles/how-mexican-cartels-are-using-drones-now-and-in-the-future/>; “Border Security: The Role of Drones in Smuggling and Surveillance,” AirSight, accessed July 7, 2026, <https://www.airsight.com/blog/border-security-drones-smuggling-surveillance>.

facility and an international airport.⁸ Domestically, foreign-made drones—overwhelmingly manufactured by China’s DJI, which controls an estimated 90 percent of the U.S. public-safety drone market—have become a national security flashpoint (see sidebar on page 14). This concern prompted the FCC to ban certain new foreign-made drone models in December 2025, even as enforcement gaps have allowed DJI technology to continue entering the market through rebranded products sold under shell company names, highlighting the challenges of translating policy into enforcement.

But together, 2025 and 2026 also saw the most significant expansion of state and local counter-drone authority in U.S. history:

- Two executive orders issued in June 2025 funded the acquisition of drone detection equipment and created the FBI’s National Counter-UAS Training Center (NCUTC) in Huntsville, Alabama.⁹
- The One Big Beautiful Bill Act, enacted in July 2025, authorized \$500 million in FEMA grants to strengthen state, local, tribal, and territorial (SLTT) counter-UAS capabilities.¹⁰
- In addition, the SAFER SKIES Act, enacted in December 2025 and implemented in July 2026 through an interim rule that took effect on July 1, 2026, extended mitigation authority beyond the four federal departments that had long held it exclusively (the U.S. Departments of Justice [DOJ], Homeland Security [DHS], Defense [DoD], and Energy [DOE]) and created for the first time a pathway for SLTT agencies to detect and—as a separate later step—to mitigate drone threats independently.¹¹

However, this new authority is neither automatic nor self-executing. To help agencies navigate this evolving environment, this report lays out two practical roadmaps for police executives.

-
8. Jon Gambrell and Samy Magdy, “Drone Strikes UAE Nuclear Plant as U.S. and Iran Signal They are Prepared to Resume War,” Associated Press, last modified May 17, 2026, <https://apnews.com/article/iran-us-uae-nuclear-drones-71e7e58f45193b7dee3df28740532a7b>; “Drone Attack Disrupts Dubai Flights as Iran Continues Gulf Attacks,” Al Jazeera, last modified March 16, 2026, <https://www.aljazeera.com/news/2026/3/16/drone-strike-disrupts-dubai-flights-as-iran-continues-gulf-attacks>.
 9. Exec. Order No. 14305, *Restoring American Airspace Sovereignty*, 90 Fed. Reg. 24719 (June 6, 2025), <https://www.whitehouse.gov/presidential-actions/2025/06/restoring-american-airspace-sovereignty/>; Exec. Order No. 14307, *Unleashing American Drone Dominance*, 90 Fed. Reg. 24727 (June 6, 2025), <https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/>.
 10. FEMA (Federal Emergency Management Agency), “Counter Unmanned Aircraft Systems Grant Program,” U.S. Department of Homeland Security, last modified June 9, 2026, <https://www.fema.gov/grants/preparedness/counter-unmanned-aircraft-systems-grant-program>.
 11. *Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies*, 91 Fed. Reg. 41466 (July 6, 2026), <https://www.govinfo.gov/app/details/FR-2026-07-06/2026-13609>.

The first roadmap is a set of eight concrete steps agencies can take now. Mitigation authority sits at the end of the sequence rather than at the beginning, and an agency that stops at detection and warning still has a working program.

1. **Build public support for C-UAS operations.** Proactively educate the community about how and why counter-UAS technology will be used, because public trust is as essential to a sustainable program as legal authority itself.
2. **Establish relationships with the key counter-UAS-specific federal agencies.** Law enforcement must establish working relationships with the UAS-specific units of the FBI field office, the Federal Aviation Administration (FAA), and the Federal Communications Commission (FCC). These relationships should include deliberate pre-incident planning to define roles and responsibilities, establish communication protocols, and develop coordinated response procedures.
3. **Determine where the C-UAS function will reside organizationally.** Decide whether counter-drone capability belongs in a real-time crime center, a fusion center, or a stand-alone unit, and clarify who is authorized to act on an alert before one occurs. This point is also where an agency should begin drafting a C-UAS implementation policy, because an adopted policy—reviewed and concurred in by agency counsel or a state or local prosecutor—is the foundation of agency accreditation under the federal rule.
4. **Plan ahead for special events.** Secure temporary flight restrictions (TFR) from the FAA and engage the regional Joint Terrorism Task Force (JTTF) well in advance of any large planned gathering, rather than treating mitigation as an afterthought.
5. **Assess critical infrastructure.** Determine which sites in the jurisdiction—including stadiums, government buildings, utilities, and transit hubs—are most vulnerable to drone threats, and prioritize preparation accordingly.
6. **Develop and implement lawful detection capabilities.** Detection now comes in two tiers. Remote ID reception, cameras, acoustic sensors, and radar require no federal certification and can be deployed today, subject to the FCC and FAA restrictions governing each. Radio frequency (RF) detection, which reads the link between a drone and its operator, delends on the SAFER SKIES Act and requires a Detection and Warning Certification for every operator, equipment drawn from the authorized lists, an adopted policy and agency accreditation, and compliance with the privacy requirements of the federal rule.
7. **Report every significant drone incident.** Submit reports through eGuardian or the local FBI field office for every suspicious drone sighting, because each report strengthens the national intelligence picture used to track emerging threats.
8. **Pursue NCUTC training and agency accreditation.** Begin with the Detection and Warning Certification, which the NCUTC delivers online at no cost and which an agency can complete now without a nomination or a training seat. Pair it with the agency's implementation policy, legal review, and portal attestation, which together establish accreditation. Mitigation is a separate and later decision. It requires the resident NCUTC course, for which the Detection and Warning Certification is a prerequisite—so agencies that intend to pursue it should begin the nomination through the local FBI field office early, because demand for seats is high.

The second roadmap is four steps for building a sustainable program once an agency is accredited and its personnel are certified:

1. **Move toward independent operations.** Transition from federal task-force deputization, which was never intended as a permanent solution, to agency accreditation, individually certified operators, authorized equipment, and independent reporting to DOJ and DHS. *Independent* here means the agency holds the authority in its own right—not that it operates without federal coordination.
2. **Develop internal policy and oversight.** Pair federal certification with the agency's own governing policy, after-action review, and compliance audits, because public support depends on how consistently and transparently the authority is used.
3. **Integrate C-UAS into existing operations.** Move detection and mitigation alerts into an established structure, such as a real-time crime center or fusion center, so that certified personnel are embedded within operations rather than working in isolation.
4. **Build sustained proficiency.** Treat mitigation readiness as a perishable skill requiring recurring exercises and ongoing coordination with the FCC and FAA, not a credential earned once and set aside.

Neither pathway will build a sustainable counter-UAS program overnight, nor will equipment purchases alone. Leadership, policy, training, and public trust will ultimately determine whether agencies are prepared to meet a threat that is growing both more common and more capable. The question facing police leaders is no longer whether malicious drones pose a clear and present danger—that question has already been answered. The question now is whether their agencies will be ready. Agencies that begin preparing today, before a crisis forces the issue, will meet that challenge; those that wait may find themselves confronting tomorrow's threats with yesterday's tools.



Introduction

The scale of unauthorized drone activity is growing rapidly, and rising numbers of law enforcement leaders view it as a public safety challenge that demands urgent attention. In May 2026, the Police Executive Research Forum (PERF) convened law enforcement executives and other stakeholders in Washington, D.C., to examine the growing threat posed by malicious use of drones. Officials pointed to a steep rise in unauthorized drone activity at major venues.

The National Football League (NFL), intensely focused on the potential for malicious drones to inflict major damage on a game-day stadium with tens of thousands of fans, reported 2,800 drone “incursions” on its stadiums during the 2025 season. The New York City Police Department (NYPD) reports an average of about 23,000 illicit drone flights *per month*. And at the University of Tennessee, the “thousands” of campus flyovers per year included a drone that hovered over the 40-yard line during a sold-out Luke Combs concert at Neyland Stadium, as shown in figure 1.

Figure 1. Attendance record–breaking Luke Combs concert at the University of Tennessee’s Neyland Stadium in 2026.



Source: “Luke Combs Breaks Neyland Stadium Concert Attendance Record,” University of Tennessee Athletics, last modified May 6, 2026, <https://utsports.com/news/2026/5/6/general-luke-combs-breaks-neyland-stadium-concert-attendance-record>.

The threat of malicious drone use is no longer distant or hypothetical. Law enforcement agencies are increasingly confronting real-world incidents that demonstrate how readily available technology could be adapted for harmful purposes. In June and July 2026, the Federal Aviation Administration (FAA) reported the seizure of more than 700 drones flying near World Cup games or fan festivals in the 11 U.S. cities hosting the soccer tournament. With a no-fly zone of three miles around the World Cup stadiums and one mile around the fan fests, the Transportation Security Administration (TSA) said in July that federal and local authorities had seized 138 drones near the Miami events, 95 in Atlanta, and 94 in Dallas.¹²

There were no reports that any of those drones had been weaponized, nor was anyone charged with any crime related to their use. But incidents like these reflect a sobering reality: If users do weaponize drones, they will likely be able to fly them into areas where they can cause significant damage if left untouched. Awareness is important, but it isn't enough. "We have the most advanced detection system in the country for our local authority," one meeting participant said, "and honestly, it's woefully inadequate."

In the seven years since PERF issued its first set of reports and warnings about the potential for unmanned aircraft systems (UAS) attacks in the United States, drone capabilities have advanced significantly, while the ability of state, local, tribal, and territorial (SLTT) police to keep pace has lagged behind. The war in Ukraine has demonstrated the lethal and versatile roles drones can play—performing raids, reconnaissance, and surveillance without endangering pilots—tactics also already being adopted by drug cartels in Mexico.



PERF May 2026 meeting to discuss the malicious use of drones in Washington, D.C.

12. FAA, "Successful Counter-Drone Efforts" (see note 1).

Until 2026, local police forces have generally lacked independent legal authority to take down a single drone. Under federal law, even small drones are generally treated as aircraft, meaning many laws that protect traditional aircraft also apply to drones. As a result, while police may be able to detect drones, they are generally prohibited from directly disabling or intercepting them. Instead, officers must find the operator to take action—or join forces with a federal agency authorized to take control of or neutralize the unidentified UAS.

But the landscape is quickly shifting. After years in which state, local, tribal, and territorial (SLTT) law enforcement agencies largely lacked the authority to directly mitigate malicious drone threats, Congress and the executive branch have begun to develop a framework to expand local capabilities. The SAFER SKIES Act¹³ established a pathway for qualified local agencies to conduct counter-UAS activities, while executive orders and federal grant programs have supported training, planning, and technology acquisition. Together, these changes represent the most significant expansion of local counter-drone authority and resources in U.S. history.

This report examines how the drone threat has evolved since PERF first warned of the risks posed by malicious drone activity in 2019; how developments in technology, criminal activity, and international conflicts have accelerated those risks; and how new federal authorities are reshaping the role of local law enforcement. Drawing on PERF's May 2026 convening of law enforcement executives, federal officials, security experts, and private-sector stakeholders as well as survey responses from nearly 270 agencies, the report explores both the emerging threat environment and the practical steps agencies can take to prepare for it.

Several overarching themes emerged from PERF's meeting and research. Together, they provide a roadmap for police executives seeking to prepare their agencies for a rapidly evolving and increasingly consequential drone threat environment.

- Malicious drone activity is no longer a hypothetical future concern; it is an increasingly common operational challenge affecting critical infrastructure, public events, correctional facilities, and criminal investigations.
- Although federal law historically limited local agencies' ability to act against unauthorized drones, legislation, executive actions, and grant funding have created a pathway toward greater local authority and capability.
- Agencies should not wait for full mitigation authority to begin preparing; building partnerships with federal stakeholders, developing policies, assessing critical infrastructure, establishing lawful detection capabilities, and pursuing training can all begin immediately.
- Effective counter-UAS programs will require not only technology and legal authority but also public trust, transparency, strong oversight, and ongoing coordination with federal partners.

In short, the question facing police leaders is no longer whether drones will affect public safety in their communities but whether their agencies will be prepared when they do. The drone threat is growing faster than the authorities, policies, and capabilities traditionally available to address it. Agencies that begin preparing now will be positioned to meet that challenge; those who wait may find themselves confronting tomorrow's threats with yesterday's tools.

13. The SAFER SKIES Act was passed as part of the National Defense Authorization Act (NDAA) for Fiscal Year 2026.



Photo courtesy The Colony (Texas) Police Department

Drone Technology— Seven Years of Change



In the seven years since PERF first turned its attention to drones, both the technology and the threat have transformed almost beyond recognition. What began as a conversation about responsible drone adoption by police departments has become an urgent question of national security.

Early Warnings About Drone Threats

By the late 2010s, police leaders were sounding the alarm about the potential for drones to inflict mass disruption and destruction. They warned urgently that federal laws barring SLTT agencies from taking direct action to mitigate suspicious drones created a significant vulnerability.

Troubling examples of malicious drone activity were popping up around the world. Drone strikes against oil facilities in Saudi Arabia in September 2019 temporarily disrupted approximately half of that kingdom's oil production capacity.¹⁴ Mexican drug cartels and ISIS terrorist groups were using drones to both attack targets and spy on law enforcement.¹⁵ And in the United States, at the 2019 Super Bowl, 10 drones were observed on game day, with one disrupting the Blue Angels flyover.¹⁶

In early 2019, PERF gathered police executives, federal stakeholders, and other experts from across the country for its first conference focused on drones. The conference explored how departments could develop and implement their own drone programs, as well as strategies for responding to malicious drone activity. By that time, many law enforcement agencies had begun

-
14. Jon Gambrell, "Saudi Arabia: Drone Attacks Knocked out Half Its Oil Supply," Associated Press, September 14, 2019, <https://apnews.com/article/d20f80188e3543bfb36d512df7777cd4>.
 15. Nathalie Guibert, "Irak: Paris Confirme Qu'un Drone Piégé a Blessé Deux Membres des Forces Spéciales Françaises à Erbil [Iraq: Paris Confirms that a Booby-Trapped Drone Wounded Two Members of French Special Forces at Erbil]," *Le Monde*, last modified October 12, 2016, https://www.lemonde.fr/proche-orient/article/2016/10/11/irak-deux-commandos-francais-gravement-blesses-a-erbil-par-un-drone-piege_5011751_3218.html.
 16. Jeff Martin, "A Deluge of Drones Fly over Super Bowl Stadium, Despite Ban," Associated Press, February 1, 2019, <https://apnews.com/article/21f228bfeee34c9a916106ebe0f1f>.

training their officers and deploying drones for a variety of uses, such as search-and-rescue missions, disaster response, crowd monitoring, traffic collision reconstruction, crime scene documentation, and investigations involving armed and dangerous suspects.

Polk County (Florida) Sheriff Grady Judd (speaking in 2019)

“During our first year and a half of operating, we’ve flown more than 750 missions, resulting in 31 suspects being arrested and five missing or endangered people being found. We are saving tens of thousands of dollars deploying drones as opposed to our piloted agency helicopters. In many situations, our drones are more versatile and effective than a helicopter.”



PERF (Police Executive Research Forum), *Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks* (Washington, DC: Office of Community Oriented Policing Services, 2020), 25, <https://www.policeforum.org/assets/Drones.pdf>.

Photo courtesy Polk County Sheriff’s Office

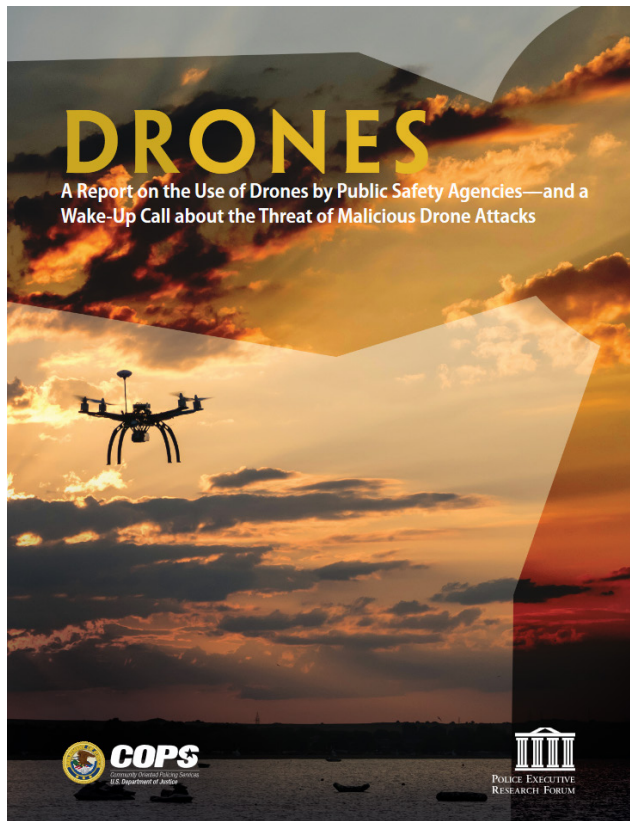
Using insights from the conference and the survey responses from 282 law enforcement agencies, PERF published *Drones: A Report on the Use of Drones by Public Safety Agencies—And a Wake-up Call about the Threat of Malicious Drone Attacks*.¹⁷ That report provided guidance on selecting and acquiring drones, establishing policies for drone teams, and mitigating drone threats.

Much of what PERF published in the *Report on the Use of Drones*, as well as the companion *Roadmap to Implementing an Effective Unmanned Aircraft System (UAS) Program*, published in 2020 in conjunction with the COPS Office,¹⁸ remains accurate and applicable today. Drone operators need to be well-trained; the laws at the local, state, and federal levels need to be well understood; coordination with the Federal Aviation Administration (FAA) and the Federal Communications Commission (FCC) is crucial; and the community’s privacy concerns must be fully addressed.

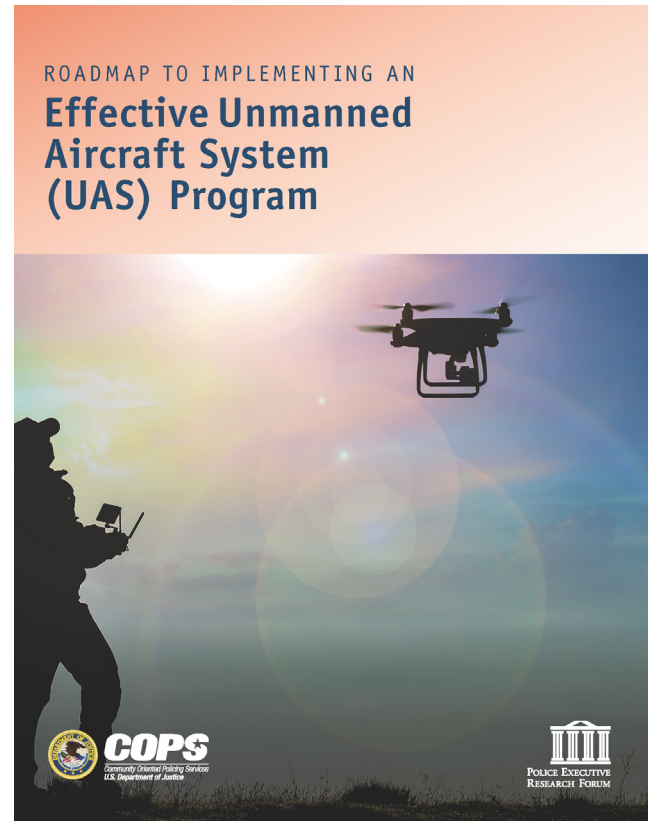
17. PERF, *Drones: A Report on the Use of Drones by Public Safety Agencies* (see note 1).

18. Lisa Mantel, *Roadmap to Implementing an Effective UAS Program* (Washington, DC: Office of Community Oriented Policing Services, 2020), <https://www.policeforum.org/assets/UASRoadmap.pdf>.

Prior PERF Publications on Drones



Drones: A Report on the Use of Drones by Public Safety Agencies



Roadmap to Implementing an Effective Unmanned Aircraft System (UAS) Program

Since those publications were released, both the number of agencies flying drones and the range of applications for that technology have grown dramatically, making drones an important tool in modern policing. However, law enforcement's ability to counter malicious drone activity has not kept pace.

"From a terrorist's standpoint, drones are accessible," NYPD Deputy Commissioner of Intelligence and Counterterrorism John Miller said in 2019. "Anyone can buy them. And they work. You don't need a suicide bomber if you can use an inanimate object to fly your bomb into your target . . . And it's repeatable; you can do this over and over again."¹⁹

Deputy Commissioner Miller and others noted then that local police were not—and still are not—permitted access to the technology needed to take down or control an unidentified drone. Police could turn to authorized federal agencies for help with large events such as games or concerts, but their routine response options remained limited. In most cases, they relied on imposing temporary flight restrictions (TFR) over designated areas and using a combination of technology alongside patrol officers to detect unauthorized drone activity and identify operators who violated the TFRs.

19. PERF, *Drones: A Report on the Use of Drones by Public Safety Agencies*, 66 (see note 1).

“So far, the United States has been lucky; we haven’t seen drone attacks,” said NYPD Chief of Department Terence Monahan in 2019, as he discussed New York’s efforts to geofence and control Times Square during New Year’s Eve celebrations. “But it’s happened around the world, so it’s something that we need to get ahead of. We need to figure out how to mitigate this threat.”²⁰

But there is hope on the horizon—**significant policy changes have expanded local law enforcement’s ability to address drone threats.**

Why Has Local Law Enforcement Historically Lacked C-UAS Authority?

Many experts argue that the safest way to mitigate the potential danger of any unauthorized craft is to assume control of it and redirect it away from people or critical infrastructure. However, as the FAA would quickly note, the national airspace includes far more than drones. Interfering with radio frequency (RF) signals carries significant risk: It could unintentionally disrupt communications or navigation systems of other aircraft, including commercial airliners, creating a serious safety hazard. Under authority delegated by Congress, the FAA treats drones exactly as it treats any other aircraft: **A drone holds the same legal status as a Boeing 767, and interfering with its radio signals is a significant safety concern.**

Chief Darin Schierbaum, Atlanta (Georgia) Police Department

“I think America has its one of its greatest vulnerabilities right now in the delivery of harm through drones.”

Additional Legal Barriers to Counter-UAS Operations

Other significant legal issues also pertain to drones. Communications between a drone operator and their flying machine are covered by federal wiretap and pen register laws, requiring a warrant or court order to intercept those signals. Similarly, according to Micheal Torphy, Assistant Section Chief of the Unmanned Aviation Section, Critical Incident Response Group, FBI, local law enforcement must be mindful of laws prohibiting computer fraud, aircraft sabotage, aircraft piracy, and satellite signal interference when dealing with an unknown drone threat. Speaking in May 2026, before the interim rule took effect, he noted that the Fourth Amendment’s prohibition of unlawful searches and seizures also applies.

The SAFER SKIES Act changed part of that picture. Section 124n(a)(12) now lifts those same statutes, along with conflicting SLTT law, for authorized actions taken by certified personnel of an accredited agency operating within the new federal rules. The relief is exactly as conditional as



20. PERF, *Drones: A Report on the Use of Drones by Public Safety Agencies*, 68 (see note 1).

the framework that carries it, and an agency operating outside those conditions remains subject to every one of those laws. The Fourth Amendment point is unchanged, and the rule carries it forward through its privacy and civil liberties requirements.

In 2018, Congress passed the Preventing Emerging Threats Act,²¹ granting the U.S. Departments of Justice (DOJ) and Homeland Security (DHS) authority to mitigate drone threats and protect specific critical infrastructure and military sites. The U.S. Department of Defense (DoD)²² and, as of the 2026 National Defense Authorization Act (section 3114),²³ the Department of Energy (DOE) hold similar but separately authorized counter-drone powers over military and nuclear-security facilities, respectively—bringing the total to four federal departments with statutory counter-UAS authority.

But until recently, local law enforcement had no authority to act. They could attempt to identify a drone via Remote ID, which generally requires registered drones to electronically broadcast identifying information.

FBI Assistant Section Chief Micheal Torphy at PERF's 2026 meeting

Referring to local law enforcement's use of Remote ID technology, "I'd say that's absolutely lawful. That's something you should have done yesterday, and it's very, very cheap, and it is somewhat effective." Remote ID, Torphy added, will only catch the "careless and clueless"—hobbyists who unintentionally stray into restricted airspace. "But that's about 99.5 percent of people that we encounter," he said, "so you have a 99 percent solution."



Local law enforcement could also use electro-optical or infrared cameras, acoustic sensors, or radar paired with cameras for identification. Radar systems can be expensive, though, and they also require coordination with the FCC or the National Telecommunications and Information Administration (NTIA)—to secure a clear spot on the spectrum—as well as with the FAA to avoid conflicting with its own radar systems. And whether the radar was passive or active, the local police were not allowed to use it to intercept communication.

The Cost of Caution

As of 2025, state and local law enforcement still had no authority to take down a malicious drone. When people saw drones over local parades, high school football games, or critical infrastructure such as water treatment facilities or power plants, police could only report these sightings to federal authorities but not take them down or even redirect them out of their own communities. The

-
21. Preventing Emerging Threats Act of 2018, Division H of the FAA Reauthorization Act of 2018, Pub. L. No. 115-254, 132 Stat. 3186, 3600 (2018) (codified as amended at 6 U.S.C. § 124n), <https://www.govinfo.gov/app/details/USCODE-2024-title6/USCODE-2024-title6-chap1-subchapII-partA-sec124n/context>.
 22. National Defense Authorization Act for Fiscal Year 2017, Pub. L. No. 114-328, § 1697(a), 130 Stat. 2000, 2639 (2016) (codified as amended at 10 U.S.C. § 130i), <https://www.govinfo.gov/app/details/USCODE-2024-title10/USCODE-2024-title10-subtitleA-partI-chap3-sec130i/context..>
 23. National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119-60, § 3114, 139 Stat. 718, 737 (2025) (protection of certain nuclear facilities and assets from unmanned aircraft), <https://www.govinfo.gov/app/details/PLAW-119publ60/related>.

primary approach available to local law enforcement has been to use each drone's unique beacon to identify the operator, then send patrol officers to that operator and instruct them to remove the drone from restricted airspace. Shooting at a drone is strongly discouraged because of the uncertainty of where a plummeting piece of machinery might land and the possibility of the drone carrying a payload—whether chemicals, drugs, explosives, or even a flame-throwing attachment.

Having located the drone operator, law enforcement had several options, including reporting them to federal databases, providing a formal warning for violating restricted airspace, seizing the drone after repeat or intentional violations, and arrest. Episodes where operators have violated airspace during NFL games have led to criminal prosecutions, FAA civil fines, or other penalties, Senior Vice President, Chief Security Officer of the NFL Cathy Lanier said at PERF's 2026 meeting (see sidebar on page 11).

As Drones Became More Capable, Concerns Intensified

All the while, drones became cheaper and more readily available and are now used on a wide variety of tasks. News media and other commercial outlets began using drones for aerial photography.²⁴ Local governments and private companies use drones to conduct aerial inspections of projects and perform topographical mapping.²⁵ Farmers and other agricultural companies are using drones to monitor crop health and to apply fertilizers and pesticides to specific targets rather than distributing them widely.²⁶ Health care companies began relying on drones to transport time-sensitive supplies such as vaccines and donor organs.²⁷ And large merchants began using drones to deliver small packages.²⁸

The U.S. military has used drones for a variety of purposes, including reconnaissance and training its own pilots. It first equipped drones with missiles in Afghanistan in 2001 and has since launched drones from submarines to provide surveillance and intelligence to the Navy.

Law Enforcement Concern is Growing Despite the Absence of a Major Attack

To date, although the potential seems to exist for a large-scale drone attack causing mass casualties, such an event has not occurred. Elsewhere in the world there have been situations where small numbers of drones caused some injuries but no fatalities;²⁹ the United States has not experienced even that. But even in this country there have been plenty of troubling incidents. In December 2023, a swarm of drones circled Joint Base Langley-Eustis in Hampton, Virginia, for 17 days,

-
24. "Drones and Journalism: Revolutionizing News Coverage or Invading Privacy?" International Association of Press Photographers, last modified October 26, 2025, <https://www.ia-pp.com/news/drones-and-journalism/>.
 25. Andrija Vidović et al., "Application of Drones in Urban Areas," *Transportation Research Procedia* 81 (2024), 84–97, <https://doi.org/10.1016/j.trpro.2024.11.010>.
 26. Ben Belton et al., "The Rapid Global Rise of Agricultural Drones: Evidence, Drivers, Impacts and an Agenda for Future Research," *Global Food Security* 48 (2026), 100897, <https://doi.org/10.1016/j.gfs.2025.100897>.
 27. Jeff Frankel, "How Drones Are Transforming EMS Logistics and Healthcare Delivery," *Journal of Emergency Medical Services*, last modified July 16, 2025, <https://www.jems.com/ems-operations/drones-transforming-ems-logistics-healthcare-delivery/>.
 28. Waylon Cunningham and Nicholas P. Brown, "Inside the U.S. Race for Drone Delivery Dominance," *Reuters*, last modified July 10, 2026, <https://www.reuters.com/business/retail-consumer/inside-us-race-drone-delivery-dominance-2026-07-10/>.
 29. "Venezuelan President Maduro Survives 'Drone Assassination Attempt,'" *BBC*, August 5, 2018, <https://www.bbc.com/news/world-latin-america-45073385>.

PERF's 2026 Meeting on Counter-UAS Authority and Malicious Drones

To address the urgency and concern law enforcement officials are sensing about the threat of drones, PERF convened approximately 150 people in Washington, D.C. in May 2026. During that meeting, police executives, top federal officials, and other stakeholders—including a Ukrainian police commander and the NFL's Senior Vice President of Security—discussed both the current malicious use of drones and the need for local counter-UAS authority.

The meeting included an intelligence briefing by the National Joint Terrorism Task Force (NJTTF) on the emerging threat of drones. It also featured a presentation by the FBI and the National Security Council on the development and implementation of legislation to grant state and local law enforcement officials counter-drone authorities and capabilities. The meeting also included discussions with law enforcement representatives from jurisdictions preparing to host the 2026 FIFA World Cup and the 2028 Summer Olympics.



PERF May 2026 meeting on the malicious use of drones in Washington, D.C.

Roughly six months prior to the meeting (and before passage of the Safer Skies Act), PERF also gathered information about the malicious use of drones and counter-UAS considerations from 269 law enforcement agencies in 40 U.S. states, Washington, D.C., and three Canadian provinces, as well as the Royal Canadian Mounted Police (RCMP).

PERF previously discussed malicious drone activities at its 2025 Town Hall gathering in Denver and at its 2026 Annual Meeting in Los Angeles and has published three reports on drones since 2020.*

* PERF, *Drones: A Report on the Use of Drones by Public Safety Agencies* (see note 1); Mantel, *Roadmap* (see note 14); PERF (Police Executive Research Forum), *Community Engagement Strategies for State, Local, Tribal, and Territorial (SLTT) Law Enforcement Unmanned Aircraft System (UAS) Programs* (Washington, DC: Office of Community Oriented Policing Services, 2022), <https://www.policeforum.org/assets/DronesCommunityEngagement.pdf>.

with neither the operator nor the intent ever identified.³⁰ More recently, unidentified drones were spotted circling over Fort McNair in Washington, D.C., in March 2026, which is troubling because the Secretary of State and the Secretary of Defense both live there.³¹

Sarasota (Florida) Police Department Chief Rex Troche at PERF's 2026 meeting



“It’s going to take one 9/11-type incident for the laws to start changing fast,” said Rex Troche, chief of the Sarasota (Florida) Police Department, “because this is this type of attack. No one’s going to see this coming . . . you could just sprinkle sugar over a crowd. Yell bomb or yell anthrax. You’re going to have a stampede, and we’re going to lose hundreds, if not thousands of people in a major incident.”

Former Sacramento (California) Police Department Chief Kathy Lester (ret.)

“The fact that, knock on wood, that hasn’t happened to one of our cities yet,” said former Sacramento (California) police Chief Kathy Lester, “is really kind of a miracle.”

The rate of malicious use of drones outside the United States gives American law enforcement even more cause for worry. The war in Ukraine has diversified drone tactics and dramatically increased their frequency in war, with both sides using drones to attack critical infrastructure, and Russia using drones to bomb civilian residential and commercial areas.



30. Dylan Thuras, “Who Swarmed Langley Air Force Base With Drones?,” Atlas Obscura, last modified June 19, 2025, <https://www.atlasobscura.com/articles/podcast-langley-air-force-base-drones>.

31. Tyler Thrasher, “Drones Spotted over DC Base where Rubio, Hegseth Live, Raising Security Concerns,” FOX 5 DC, last updated March 19, 2026, <https://www.fox5dc.com/news/drones-dc-base-rubio-hegseth-security>.

Serhii Bolvinov, Deputy Chief of the Kyiv Regional Police, described how Iranian drones once used mainly for reconnaissance now “identify targets, adjust fire, strike mine roads, pursue vehicles, and terrorize civilians.” He also described how Russian drones are now using fiber-optic cables, sometimes miles long, to control drones without radio frequencies, so they cannot be intercepted by standard RF mitigation tactics. The *Washington Post* recently reported that a 12-year-old Ukrainian boy perched in a tree disrupted a potentially fatal attack by grabbing a drone’s cable and tying it in knots.³² For more on the drone-related implications of the war in Ukraine, see the sidebar on page 16–17.



Deputy Chief of the Kyiv Regional Police Serhii Bolvinov

And in Mexico, drug cartels have been using weaponized drones against rival cartels, security forces, and even civilian communities since at least 2020, according to a recent report from the Brookings Institution.³³ Large numbers of drones are used to attack competing drug labs or even to carpet bomb rural areas to render them unusable for competing drug production. The head of U.S. Northern Command testified to Congress in 2024 that there were more than 1,000 incursions by Mexican drones each month on suspected reconnaissance or drug smuggling missions. An off-the-shelf drone loaded with a primitive explosive device infiltrated a state prosecutor’s compound in Tijuana in October 2025, killing no one but showing that such devices could effectively penetrate even highly protected areas.³⁴

32. Steve Hendrix and Kostiantyn Kudov, “In Northern Ukraine, It Was Boy vs. Russian Drone. The Boy Won,” *Washington Post*, May 15, 2026, <https://www.washingtonpost.com/world/2026/05/15/russian-drones-hunt-ukrainians-human-safari-boy-fought-back/>.

33. Felbab-Brown, “How Mexican Cartels are Using Drones” (see note 7).

34. David Martin Davies, “Mexican Drug Cartels Use of Weaponized Drones Causing Concern on the Border,” Texas Public Radio, last modified March 2, 2026, <https://www.tpr.org/border-immigration/2026-03-02/mexican-drug-cartels-use-of-weaponized-drones-causing-concern-on-the-border>.



“We need to be running towards solutions, not walking,” said Lisa Davis, chief of the Austin (Texas) Police Department. “This is something that needs to be addressed immediately.”

Chinese Manufacturer Leads the Market . . . For Now

Shenzhen-based DJI leads the global drone market and is estimated to control approximately 90 percent of the global consumer drone market, about 75 percent of the U.S. market, and as much as 90 percent of drones used by American public safety agencies as of July 2026. That dominance has made DJI the focal point of the broader debate over foreign-made drones in the United States.

In January 2025, just days after the United States proposed a rule that would effectively prohibit new DJI drones from entering the American market, the company announced it would remove geofencing—the technology that had automatically restricted its drones from flying over airports, military installations, and other sensitive locations.* DJI said the feature, originally intended to promote responsible flight practices and educate users about airspace restrictions, was no longer necessary given advances in regulatory awareness and aviation technology, and that removing it would return greater control to operators.

DJI has pushed back on the ban and petitioned for reconsideration. In May 2026, it released the results of a security audit done by the U.S. cybersecurity firm OnDefend that found no vulnerabilities in hardware, firmware, software, or radio frequency testing; no data sent outside the United States; and no pathways for hijacking or weaponization.† The ban on new DJI models nevertheless remains in place as of the publication of this report.

* Jim Moore, “DJI Replaces Geofences With Advisories,” AOPA News, January 23, 2025, <https://www.aopa.org/news-and-media/all-news/2025/january/23/dji-replaces-geofences-with-advisories>.

† Haye Kesteloo, “DJI’s New U.S. Security Audit By OnDefend Finds No Backdoors, No Foreign Data Transmission In Air 3S And Matrice 4E,” DroneXL, last modified May 28, 2026, <https://dronexl.co/2026/05/28/dji-ondefend-security-audit-air-3s-matrice-4e/>.

The Growing Risk of Malicious Drone Operations



The easy availability of drones and their ability to spray chemicals, drop payloads, and fire weapons have greatly increased their potential to inflict chaos and carnage—and increased the urgency for American law enforcement to be ready.

Highly capable and inexpensive consumer drones are readily available, as are online instructions for modifying them for malicious purposes. Consumer drones with video capability can be purchased for well under \$100. People are now using drones with pressure washing capability to clean buildings and wash windows, while farmers are using drones to spread fertilizer. An attachment to enable a drone to have flame-throwing capability—“for industrial, agricultural, *and entertainment* applications” (emphasis added)—is available online for \$1,600.

While drones have innumerable legitimate uses, misuse poses a genuine threat. In April 2026, a truckload of 15 giant agricultural drones, each the size of an all-terrain vehicle, was stolen in New Jersey.³⁵ The drones could carry and spray up to 40 gallons of liquid chemicals, such as fertilizers and pesticides, over a 15-acre span in just seven minutes. A month later, the drones were found, untouched, in a New Jersey warehouse.³⁶ Whether the truckload was stolen or mistakenly delivered to the wrong place has not been disclosed.

Commercially made drones are required to have a registered operator and a locator beacon. But do-it-yourself drones—built from freely available online instructions—are increasingly common, and the implications are troubling. 3D printers can also be used to produce drone components, evading registration and location requirements altogether, and a DIY can be built very affordably.

-
35. Shane Galvin, “15 Chemical Spraying Drones Stolen in NJ as FBI Investigates Possible ‘Nightmare Scenario’: Report,” *New York Post*, April 25, 2026, <https://nypost.com/2026/04/25/us-news/15-chemical-spraying-drones-stolen-in-nj-as-fbi-investigates-possible-nightmare-scenario-report/>.
36. “Stolen Agricultural Drones Recovered at New Jersey Warehouse,” 6abc Action News Philadelphia, last modified April 28, 2026, <https://6abc.com/post/stolen-agricultural-drones-recovered-new-jersey-warehouse/18985482/>.

The War in Ukraine has accelerated the “arms race” between drones and C-UAS measures

Russia’s invasion of Ukraine in February 2022 has transformed both modern warfare and the use of drones for offensive and defensive operations. The rapid evolution of drone technology and tactics has been especially striking. As Serhii Bolvinov, First Deputy Chief of the Kyiv Regional Police, noted at the PERF meeting in May, “The war in 2022 and the war today are already two different wars.”

Bolvinov noted that Russia began deploying drones not only along the front lines but also deep behind them, a tactic Ukraine also subsequently adopted. He highlighted the evolution of the Iranian-manufactured Shahed drone, which was once mainly associated with reconnaissance but has become “a full-scale instrument of war.” Russia now uses the drones to strike supply lines and terrorize civilian populations. As a result, Bolvinov said, his department investigates every drone strike targeting civilians as a potential war crime.



Deputy Chief of the Kyiv Regional Police Serhii Bolvinov speaks at PERF’s 2026 meeting

Ukraine employs a variety of counter-UAS methods, Bolvinov said, including using interceptor drones, shooting down enemy drones, and installing protective netting over civilian areas to help disrupt drone strikes. Some drones can also be programmed with GPS coordinates and sent directly to a target in a kamikaze-style self-destruct attack, requiring no radio communications. So both Russia and Ukraine have begun using “spoofing” techniques, which disrupt navigation by transmitting false location data and redirecting drones away from them. According to Defense News, Russian spoofing operations have diverted Ukrainian drones into NATO airspace, while Ukrainian countermeasures have redirected Russian drones into open fields or back toward Russian territory.*

To counter GPS spoofing or radio-frequency interception, Russia has increasingly deployed drones connected to operators via long fiber-optic cables, eliminating the need for radio communication, Bolvinov said. Because the control signals travel through a physical cable rather than radio frequencies, these drones are largely immune to electronic jamming and interception. The Kyiv police commander showed a photo of a Ukrainian neighborhood draped in shining fiber-optic strands, which can reach for many miles, as shown in figure A1.

Figure A1. A Ukrainian neighborhood covered with Russian fiber-optic drone cabling



Photo: 3-тя Окрема Штурмова Бригада [3-tia Okrema Shturmova Bryhadal] (3rd Separate Assault Brigade, Ukrainian Ground Forces).

Yet the police are still trying to do their jobs. “Today, police officers in Ukraine work under an almost constant aerial threat,” Bolvinov said. “We continue to perform regular police duties, responding to crimes, maintaining public order, investigating war crimes and helping people. But now even a routine deployment can take place under the risk of double-tap strike.”

* Katie Livingstone, “How Russia is Turning Ukraine’s Drones against NATO,” Defense News, May 29, 2026, <https://www.defensenews.com/global/europe/2026/05/29/how-russia-is-turning-ukraines-drones-against-nato/>.

Concerns about Foreign-Made Drones

As drones have become ubiquitous across the United States, so have concerns about the national security risks posed by foreign-made models—particularly those manufactured in China, which has come to dominate the global drone market (see *Chinese Manufacturing* sidebar on page 14). U.S. policymakers and security officials have warned that data collected by foreign-manufactured drones could be accessed by adversarial governments or that the drones themselves could be vulnerable to unauthorized remote control or other forms of interference.

On December 22, 2025, the FCC added foreign-made drones and critical drone components to its Covered List³⁷ following a federal national security review that concluded such equipment posed “unacceptable risk to the national security of the United States.”³⁸ As a consequence of that listing, newly manufactured foreign-made drone models generally can no longer obtain the FCC equipment authorizations required for lawful sale in the United States. But that action does not apply retroactively: Drones that had already received FCC authorization or were already in operation before the rule took effect are still permissible to use. Nevertheless, owners of those legacy systems may face growing challenges over time as access to replacement parts, software updates, maintenance services, and technical support becomes scarce.

Agencies seeking alternatives have many options that comply with the National Defense Authorization Act (NDAA) and need not be American-made. NDAA-compliant drones must not contain critical components from countries specifically covered by the NDAA—China, Russia, Iran, and North Korea—and manufacturers must demonstrate a transparent supply chain.

The DoD has created a “Blue UAS” program that assesses drones for compliance, and federal agencies are required to use drones from the Blue UAS List. According to the website UAV Coach, as of this writing, there are nine drone companies with 16 drones on the list.³⁹

Increasing International Use of Drones for Criminal Activity

Organized criminal groups in other countries have also begun using drones for malicious purposes, sometimes in sophisticated ways. Mexican drug cartels, in addition to using drones to scout the U.S. border as well as rival turf, have used custom-built agricultural drones capable of transporting payloads up to 220 pounds and making precision deliveries.⁴⁰ Various organized crime groups have also started using maritime drones—or unmanned underwater vehicles (UUV)—to move loads of cocaine on shallow routes along coastlines, from Latin America to Europe, where radar cannot detect them, according to the Brookings Institution.⁴¹

37. Federal Communications Commission, “List of Equipment and Services Covered By Section 2 of The Secure Networks Act,” last modified July 21, 2026, <https://www.fcc.gov/supplychain/coveredlist>.

38. Dana Nickel, “FCC Bans Foreign-Made Drones over National Security, Spying Concerns,” *Politico*, December 22, 2025, <https://www.politico.com/news/2025/12/22/fcc-drone-ban-dji-00703742>.

39. UAV Coach, “Blue UAS: The Full List of DOD Approved ‘Blue Drones,’” accessed July 8, 2026, <https://uavcoach.com/blue-uas/#guide-2>.

40. “Border Security” (see note 7).

41. Felbab-Brown, “How Mexican Cartels are Using Drones” (see note 7).

The potential for drone attacks from Mexico caused a major incident in El Paso, Texas, in February 2026. While Customs and Border Patrol was flying a drone near the Fort Hancock area, the DoD used a laser to shoot it down. The takedown had not been approved by the FAA, which briefly grounded flights at the El Paso airport and imposed airspace closures, while lawmakers expressed frustration over the breakdown in interagency communication.⁴² The Pentagon issued a statement saying “the engagement took place far away from populated areas and there were no commercial aircraft in the vicinity.”⁴³

Threat Briefing from the National Joint Terrorism Task Force (NJTTF)

Intelligence analysts from the National Joint Terrorism Task Force spoke at the 2026 PERF meeting and provided a law enforcement–sensitive presentation on threats posed by UASs. Much of their full briefing cannot be reproduced in a public-facing report; however, non-sensitive portions of their presentation are summarized here.

They encouraged agencies to report all suspicious drone sightings to the federal eGuardian system. They also urged law enforcement to use the NJTTF’s Unmanned Aerial Systems Response Playbook both to report drones and to respond to them. For more detailed information on reporting drone activity, see the sidebar UAS Incident Reporting Checklist on page 40.

Most drone reports come from along the east and west coastlines, particularly in port areas, but other potential targets include military bases, government facilities, transportation hubs, and energy production sites such as nuclear facilities and hydroelectric dams. The FBI has counter-UAS coordinators in every field office to assist local police.

Other takeaways from their presentation were the following:

- The Bureau of Prisons (BOP) has seen a huge uptick in drone incursions, roughly five to eight per week, attempting to deliver drugs, cell phones, and tobacco to incarcerated individuals. The growing spread of data centers adds another potential target for malicious drones.
- Drones are adding geolocation capacities, increasing their autonomy and making detection more challenging. DIY drones are often harder to locate, particularly those built from 3D-printed components using software downloaded from the internet. Drones controlled through fiber-optic cables can be especially difficult to counter because they do not rely on radio frequency communications. In Ukraine, dozens of drones have been launched simultaneously from the back of a single truck.
- Terrorists and domestic extremists are interested in drones as attack platforms. ISIS has threatened to use drones against major U.S. cities, and federal authorities have disrupted plots involving drones targeting civilian and military sites in several cities. Military bases have reported multiple fly-over incursions around the country, but only 12 percent of the operators have been located, and detection systems have worked less than half the time.
- The intelligence community has determined that drone activity and drone weaponization are increasing. Greater public awareness and vigilance will naturally lead to some rise in reporting; nevertheless, the increase in malicious use and adaptation and destructive drone payloads is very real. One government official noted that the bad actors may be innovating faster than the mitigators can keep up.

42. Clara McMichael and Ayesha Ali, “Dept. of Defense Shoots Down Customs and Border Protection Drone Near El Paso: Officials,” ABC News, last modified February 27, 2026, <https://abcnews.com/US/dept-defense-shoots-customs-border-protection-drone-el/story?id=130548708>.

43. Pete Muntean, Alexandra Skores, and Katherine Dautrich, “Pentagon Shoots Down U.S. Customs and Border Protection Drone with Laser System, Lawmakers Say,” CNN, last modified February 27, 2026, <https://www.cnn.com/2026/02/26/us/pentagon-shoots-down-cbp-drone>.

According to federal officials at PERF's meeting, drone attacks have occurred in Africa: Rwandan-backed rebels used drones to target an airport in Congo;⁴⁴ suspected Islamist terrorists used drones to attack a military base in Niger;⁴⁵ and the Ethiopian government used drones to target an airport in Sudan that had just reopened after three years.⁴⁶

The United Arab Emirates (UAE) began facing large-scale drone attacks in March 2026, after the United States and Israel launched a war with Iran, said Mohammed Bin Jumah, from the UAE Ministry of the Interior, at the 2026 PERF meeting. Bin Jumah said 2,260 drones had been launched into the UAE as of May, most of them successfully intercepted. Drone and missile strikes near the Dubai airport caused injuries and property damage on several occasions;⁴⁷ in May, drone strikes caused a major fire at an oil facility, while a drone ignited a fire outside the perimeter of the nuclear plant in Barakah.⁴⁸

The UAE is not alone. "Drone and missile attacks [have] struck refineries and [natural gas] plants in Saudi Arabia, Kuwait, and Qatar" since the start of the war.⁴⁹



Mohammed Bin Jumah, from the UAE's Ministry of the Interior, speaks at PERF's 2026 meeting

-
44. "Rebels Claim Drone Attack on Congo's Kinsangani Airport," Reuters, last modified March 2, 2026, <https://www.reuters.com/world/africa/congos-kisangani-airport-attacked-by-suspected-rebel-drones-authorities-say-2026-03-02/>.
 45. "Niamey Airport Attack: Islamic State Claims Responsibility," African Security Analysis, last modified January 31, 2026 ("SITE Intelligence Group reported that IS fighters conducted the operation against the military base located inside the airport complex"), <https://www.africansecurityanalysis.com/updates/niamey-airport-attack-islamic-state-claims-responsibility>.
 46. Basillioh Rukanga, "Sudan Accuses Ethiopia and UAE of Orchestrating Drone Attacks on Airport," BBC, last modified May 6, 2026, <https://www.bbc.com/news/articles/clype712r3qp>.
 47. "Drone Attack Disrupts Dubai Flights" (see note 8).
 48. Gambrell and Magdy, "Drone Strikes UAE Nuclear Plant" (see note 8).
 49. Sudev Kidaya and Sumanta Sen, "Attacks on Major Oil, Gas Sites in the Middle East," Maps and Charts of the Iran War, Reuters, last modified March 20, 2026, <https://www.reuters.com/graphics/IRAN-CRISIS/MAPS/znpnmelervl/>.

“We had a large-scale burglary pattern targeting Asian business owners’ homes where the suspects were actively using drones for surveillance and reconnaissance of targets and as overwatch during the burglaries.”



The Increasing Domestic Use of Drones for Criminal Activity

Many meeting participants expressed astonishment that the United States has not yet had a significant malicious drone attack. However, the threat is very real, and most attributed the absence of such an attack to pure luck. And although the United States has not experienced the type of state-level attacks that have taken place in other countries,⁵⁰ law enforcement agencies are seeing drones used in more routine criminal activity. Examples of domestic criminal activity involving drones were mentioned during the 2026 PERF meeting and in the pre-meeting questionnaire:

“We are aware that motor vehicle thieves are utilizing drones for pre-theft surveillance. This is another driving factor behind acquiring drone detection and identification equipment.”

Lieutenant Brandon Roy, City of Warren (Michigan) Police Department

“One of our UASs was shot at and hit during a police operation. We worked with our federal partners to find the responsible party, but the DA and AUSA declined to prosecute.”

Sergeant Nic Fox, Sacramento (California) Police Department

“We have intercepted a drone trying to drop contraband into our county jail. We also have confiscated drones during events where we obtained a temporary flight restriction.”

Deputy Chief Charles Hampton, Jr., Atlanta (Georgia) Police Department

50. Amnesty International reported in June that drone strikes in the spring on civilian targets in Gulf Cooperation Council countries such as Bahrain, Saudi Arabia, and the UAE show strong evidence of having been perpetrated by the government of Iran. Conversely, in August 2025 a dozen police officers were killed in Colombia when, according to that country’s defense minister, a guerilla group used a drone to attack, disable, and crash the helicopter they were flying on an anti-drug sortie. “Iran: Deadly Drone Strikes on Bahrain and Saudi Arabia may Constitute War Crimes—New Research,” Amnesty International, last modified June 18, 2026, <https://www.amnesty.org/en/latest/news/2026/06/iran-deadly-drone-strikes-on-bahrain-and-saudi-arabia-may-constitute-war-crimes-new-research/>; Leonardo Rocha and Yang Tian, “At Least 18 Killed and Dozens Injured in Separate Colombia Attacks,” BBC, last modified August 21, 2025, <https://www.bbc.com/news/articles/cwypw0xvdk5o>.

In Washington Township, Pennsylvania, a man used a drone to drop homemade nail bombs on his ex-girlfriend's property.⁵¹ In Utah, a couple used a drone to spy on people in their homes.⁵² In a July 2025 join statement to the Senate Judiciary Committee, FBI Assistant Section Chief Torphy and Christopher Hardee of the FBI described a man in Los Angeles who used a drone to deliver fentanyl and other narcotics to buyers, one of whom died of an overdose.⁵³

Prisons and jails are regularly targeted for contraband drops, and many have limited counter-drone resources, though the DOJ statement said the BOP has installed drone detection systems at 64 of its 121 federal facilities. The 474 incursions and sightings reported by the BOP in 2024 were 20 times the number reported in 2018.

International Events Hosted in the United States

At the time of PERF's meeting in May 2026, law enforcement and first responders at all levels—from the smallest police department to the FBI—were preparing for three large-scale events that posed the potential for malicious drone incursions.

The first was the FIFA 2026 World Cup in June and July, staged in 11 cities around the United States, as well as two in Canada and three in Mexico. Police officials noted that in addition to the games themselves, "Fan Fests" are often held for days in the cities hosting the games, requiring security accommodations and drone preparedness. Police departments in each of the American World Cup host cities received advance training from the FBI's National Counter-UAS Training Center (NCUTC) in Huntsville, Alabama (see sidebar on page 29), which was established in 2025 to train and coordinate counter-drone activities ahead of the World Cup and is now training police officers from around the country.

As the World Cup approached, federal authorities moved to reassure community members that they had shown the capability to fend off drone incursions at other large-scale events and reiterated the existence of no-fly zones around World Cup events. Homeland Security Secretary Markwayne Mullin told Congress that federal officers had successfully dealt with other events in 2026, including taking down eight drones over a Formula 1 race in Miami and 12 drones that entered the no-fly zone over the Masters golf tournament.⁵⁴

But "everybody's a little behind" the rapidly evolving technology, Mullin said. "Biggest concern I have is honestly with drones," Mullin said. "I wouldn't say a vulnerability, but it is one of the areas that we are struggling with every day."

51. "Pennsylvania Man Allegedly Used Drone to Drop Explosives on House," AirSight, accessed July 8, 2026, <https://www.airsight.com/en/news/pennsylvania-man-allegedly-used-drone-to-drop-explosives-on-house>.

52. Nick Bilton, "When Your Neighbor's Drone Pays an Unwelcome Visit," *The New York Times*, January 27, 2016, <https://www.nytimes.com/2016/01/28/style/when-your-neighbors-drone-pays-an-unwelcome-visit.html>.

53. Christopher Hardee and Micheal Torphy, "Statement of Christopher Hardee and Micheal Torphy to the Senate Judiciary Committee," Testimony, Federal Bureau of Investigation, July 22, 2025, <https://www.fbi.gov/news/speeches-and-testimony/statement-of-christopher-hardee-and-micheal-torphy-to-the-senate-judiciary-committee>.

54. Josh Funk, "At World Cup Stadiums, There Will Be Zero Tolerance for Drones Because of the Threat They Pose," Associated Press, last modified June 10, 2026, <https://apnews.com/article/world-cup-drones-threat-fbi-war-ukraine-6583988184f5075d487478bff015bbd1>.

Although the World Cup concluded without a catastrophic incident, it provided a stark reminder of the persistence of the drone threat. Federal and local authorities reported seizing more than 700 drones operating near World Cup stadiums and fan festivals, demonstrating that unauthorized drone activity remains commonplace even during heavily secured events.⁵⁵

Later this year PERF will be releasing a publication about how three cities—Atlanta, Kansas City, and Philadelphia—prepared for and managed their World Cup experience. All three cities sent personnel to the NCUTC in Alabama and developed counter-drone capabilities and strategies before hosting the games.

Also attracting attention were the America250 and Freedom 250 celebrations marking the United States’s 250th anniversary, or semiquincentennial. Various events took place nationwide, including New York City, although the largest occurred in Washington, D.C.

Like the 2026 World Cup, the America250 celebrations concluded without a major drone-related security incident. Prior to the events, however, the FAA treated unauthorized drone operations as a significant concern, establishing No Drone Zones around many America250 events and distributing a national communications toolkit to help federal, state, local, and private sector partners educate the public about drone restrictions and penalties for violations.⁵⁶ Authorities also publicly warned that unauthorized drone activity could result in fines, criminal charges, and the seizure of the aircraft.⁵⁷

In July 2028, the Summer Olympics are returning to the United States and will be held in the Los Angeles area and Oklahoma City. Police departments in those areas are expected to engage with federal agencies to obtain authorization and training to detect and mitigate malicious drones.



Atlanta’s Mercedes-Benz Stadium seen from above during a 2026 World Cup match

55. Kelly O’Donnell and Michael Kosnar, “FBI Has Seized More Than 600 Drones Near World Cup Events,” NBC News, last modified July 4, 2026, <https://www.nbcnews.com/sports/soccer/fbi-seized-600-drones-world-cup-events-rcna353006>.

56. FAA (Federal Aviation Administration), “America250: No Drone Zone Toolkit,” U.S. Department of Transportation, last modified May 15, 2026, https://www.faa.gov/america250/no_drone_zone.

57. Jessica Kronzer, “Security Plans for July Fourth Fireworks, More Freedom 250 Events in DC,” WTOP News, last modified June 2, 2026, <https://wtop.com/dc/2026/06/security-plans-for-july-fourth-fireworks-more-freedom-250-events-in-dc/>.

A Dozen Drones a Game: Securing America's Stadiums

Since 2021, every NFL stadium has been required to deploy technology capable of detecting, tracking, and locating drones on game days. Yet despite those measures, unauthorized drone activity remains a persistent challenge. NFL Chief Security Officer Cathy Lanier said that security teams deal with “at least a dozen [drone incursions] every single game [forcing] ground intercept teams” to quickly identify operators and intervene before the aircraft can threaten fans, players, or stadium operations.

As the law stands now, each use of FBI counter-UAS operations must be approved by the Deputy Attorney General. But Lanier has been at the forefront of pushing Congress and federal regulators to give local police the authority to not just detect but take down the drones themselves. “The drone threat has really, really taken off,” Lanier said, “and we are still waiting for this authority to expand so that we can have it for large mass gatherings across the United States.”*

Starting in 2019, the NFL has worked with the FBI to take down drones outside the Super Bowl, and it did so again at the 2026 NFL Draft in Pittsburgh, where more than 800,000 people gathered outside over three days. The NFL applied for a TFR from 11:00 a.m. to midnight on each of those days, during which no drone was permitted to enter. Once a drone violates restricted airspace, “the counter-drone teams will either take control of the drone and take it to a landing zone, or they’ll mitigate it some other way,” Lanier said. In this instance, mitigation meant redirecting drones toward the river adjacent to the NFL draft site, rather than tracking down the operator.

The Super Bowls have been the only NFL games where FBI teams with “mitigation authority” have deployed, but the league can still be vigilant about monitoring the airspace around stadiums. So for every game, regular and post-season, the NFL obtains approval from the FAA for a TFR around each stadium.

“Having a good relationship with the FAA is also very important,” Lanier said. For the NFL, “the FAA is critical” because it helps manage authorized drones used by television broadcasters and helps determine who is violating a TFR.

Once a TFR is in place, “detect, track, and locate” technologies are used to spot an unauthorized drone, Lanier said. “Once a drone is detected, it automatically connects with the stadium camera, [which] turns in the direction of the drone so we can get a look at that drone.” Trained agents then use the drone’s identifiers to determine its size and potential payload.

“On average, the last two years,” Lanier said, “we’ve had 2,800 drones that have violated our TFR during the NFL regular season alone.” She credited state and local law enforcement, whose ground intercept teams track down drone operators, with doing “an amazing job every single NFL game.”

But the NFL isn't the only league drawing huge crowds every weekend. College football stadiums on Saturdays often have larger capacities than the NFL, as well as large crowds outside. "I had thousands of drone incursions over my campus last year," said University of Tennessee Police Chief Sean Patterson, "so they are definitely going to surveil critical infrastructure."

Patterson also discussed a recent Luke Combs concert in Neyland Stadium. "We had a drone at the 40-yard-line that was not part of production, that was not picked up by the current software we have," he said, noting it also would not have been caught by newer software the school plans to use in the future. "That could have something as simple as a grenade on it. My stadium's over 100 years old; I'm not getting those 80,000 people out." He said if terrorists "want to do the most effective damage, they're going after my facilities, or [NFL] facilities, or MLB or NASCAR, because that is going to be the most carnage . . . that is the easiest thing for them to get."

At the University of Notre Dame, in addition to 80,000 fans watching the Fighting Irish, the games attract "another 20,000 people who never come into the stadium," University Police Deputy Chief William Thompson said. He and other departments said they use Dedrone counter-drone detection software. But "what concerns me a lot," Thompson said, "is the time frame of detection to having to put a mitigation plan into effect. We're talking minutes. We might be talking seconds. It is literally 300 yards from the south wall of my stadium across the city line to parking lots where people could launch anything."

Lieutenant Kevin Crowley from the University of Michigan Police Department said state agencies have "created a drone association" for all local law enforcement and first responder agencies, and the detection information from about 32 agencies is being integrated by a third-party vendor. "We're able to see each agency's detection software, regardless of company," Crowley said, "for real-time live flight operations."

The Michigan association is also hoping to launch a historical search function of the various agencies' drone detections, Crowley said. "So if I had a flight on the Ann Arbor campus, I could search that serial number," he said. "I may see its activity in Comerica Park in Detroit, maybe out in East Lansing or the Grand Rapids area. [Those] are some of our big areas right now that we're trying to share that information at a state level, at least."

Assistant FBI Section Chief Micheal Torphy of the bureau's Unmanned Aviation Section said that "in traditional security culture, the more gates and more guns you have, the more protected you are from the traditional attack methodologies, but the more vulnerable you are to attack from above. In fact, now your hardest targets are actually not necessarily the easiest to hit, but they're the most likely to be hit from the sky."

* Cathy Lanier, "Statement of Cathy L. Lanier, Chief of Security, National Football League, before the Subcommittee on Counterterrorism, Law Enforcement, and Intelligence; Subcommittee on Transportation and Maritime Security Subcommittee; Committee on Homeland Security; United States House of Representatives," December 10, 2024, <https://www.congress.gov/118/meeting/house/117754/witnesses/HHRG-118-HM05-Wstate-LanierC-20241210.pdf>.



Photo courtesy Hemet (California) Police Department

Recent Changes to Resources and Authority



In 2025, things began to change for local police and their drone-fighting capability. On June 6, 2025, President Trump signed two EOs. The first, *Restoring American Airspace Sovereignty*,⁵⁸ authorized federal grants for counter-UAS detection by SLTT agencies and established the new NCUTC. That order expanded agencies' capacity to *detect* threats, but it did not grant them new authority to take down or *disable* drones. The second, *Unleashing American Drone Dominance*,⁵⁹ focused primarily on building up the U.S. domestic drone manufacturing industry, while also expanding beyond-visual-line-of-sight (BVLOS) drone operations and accelerating the integration of private drones into the national airspace.

In July 2025, Congress passed the One Big Beautiful Bill (OB BB) Act, which allocated \$500 million in grants to support counter-UAS capability for SLTT agencies.⁶⁰ Then in December 2025, with the passage of the SAFER SKIES Act, Congress created a pathway for SLTT agencies to obtain mitigation authority previously reserved only to four federal departments.⁶¹

The following sections present a more detailed look at how those federal-level moves have significantly expanded opportunities for SLTT agencies to create their own mitigation programs.

Executive Orders

EO 14305, *Restoring American Airspace Sovereignty* (see note 9), focused on accelerating counter-drone capabilities for state and local police to protect public safety and critical infrastructure. It also established a task force to review regulatory frameworks and propose solutions to UAS threats and created the possibility for larger no-fly zones and geofencing around critical infrastructure sites. The order also directed the FAA to “promptly” implement section 2209 of the FAA Extension,

58. Exec. Order No. 14305 (see note 9).

59. Exec. Order No. 14307 (see note 9).

60. FEMA, “Counter Unmanned Aircraft Systems Grant Program” (see note 10).

61. National Defense Authorization Act For Fiscal Year 2026 (see note 23).

Safety, and Security Act of 2016⁶²—a nearly decade-overdue statutory mandate. **The FAA’s proposed rule, published May 6, 2026, would allow owners of critical infrastructure, such as power plants, prisons, and stadiums, to petition for a formally designated no-fly zone over their sites.** The rule does not itself expand detection or mitigation authority—that remains governed separately by the SAFER SKIES Act—and it remained open for public comment through August 5, 2026.

EO 14305 further instructed that DOJ and DHS permit SLTT agencies to receive grants to purchase drones and equipment for tracking drones. It also directed the Attorney General and Secretary of Homeland Security to explore integrating counter-UAS operations into regional Joint Terrorism Task Forces (JTTF). And it created the NCUTC, specifying that initial training should focus on securing events such as the 2026 World Cup and 2028 Summer Olympics.

EO 14307, *Unleashing American Drone Dominance* (see note 9), focused on building up the U.S. domestic drone manufacturing industry rather than on expanding law enforcement authority. This EO directed the Secretary of Commerce to prioritize drone exports and reduce foreign trade barriers and instructed the DoD to prioritize procurement of U.S.-manufactured drones for military use. It also expanded BVLOS drone operations—allowing pilots to fly drones outside their direct line of sight, a capability used in drone-as-first-responder programs, search and rescue, and disaster response—and established a pilot program for electric vertical takeoff and landing (eVTOL) aircraft integration.

Funding through the DHS/FEMA C-UAS Grant Programs

The OBBB Act authorized a \$500 million grant program administered by DHS/FEMA to support SLTT C-UAS capability development. A second tranche of grants is forthcoming in FY 2027 in which agencies in all 50 states, Washington, D.C., and all five territories will be eligible. Agencies must apply for funding through each state or territory’s State Administrative Agency, which is required to pass through at least 97 percent of awarded funds to local and tribal subrecipients.

There are five eligible activity categories for grants:

1. **Planning.** UAS response plans, standard operating procedures, coordination protocols
2. **Organization.** Regional task forces, interagency structures
3. **Equipment.** Detection systems, sensor fusion, networking
4. **Training.** FBI NCUTC attendance, system-specific training
5. **Exercises.** Tabletop, functional, and full-scale

Notably, the Notice of Funding Opportunity (NOFO) requires FEMA to verify that an agency has registered for or completed NCUTC training before mitigation equipment—as opposed to detection or tracking equipment—can be purchased.

62. FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114-190, § 2209, 130 Stat. 615, 634–635 (2016), <https://www.govinfo.gov/app/details/PLAW-114publ190/summary>.

An Inside Look at the FBI's National Counter-UAS Training Center in Huntsville, Alabama

The National Counter-UAS Training Center (NCUTC) opened in early November 2025 at Redstone Arsenal, the U.S. Army installation in Huntsville, Alabama, where the FBI has long maintained training facilities. It is intended for SLTT law enforcement personnel to learn how to safely detect, track, and mitigate unauthorized drones.

At the PERF meeting, FBI Assistant Section Chief Torphy discussed how the center works. Each class has 16 students, who take about 80 hours of instruction over two weeks. The instructional costs are covered by the FBI, and many of the center's early students were law enforcement personnel from the 11 U.S. World Cup cities.

The course focuses on temporary special-event protection, ad hoc deployments, equipment setup, integration, operation, and troubleshooting. The course also gives the students broad technical exposure to a variety of types of drones and encourages inter-agency cooperation as the FBI attempts to establish an interoperable national standard.

Before the interim rule took effect on July 1, 2026, graduates could take mitigation action only while deputized on a federal task force. That is no longer the only path. Graduates hold an individual Mitigation Certificate and may operate under their own agency's authority once that agency is accredited, and deputation remains available for task for operations. (A person executing a mitigation operation must also hold a current FAA part 107 remote pilot certificate.) The course does not certify an entire department, nor does it "train the trainers," that is, certify graduates to train others. The course also does not provide UAS flight training—attendees are expected already to have that skill—nor does it focus on permanent or long-term site protection. Also not provided is deep vendor-specific training or a focus on kinetic systems of mitigation, such as net captures.

Attendees must hold a current Detection and Warning Certification before starting the classes at NCUTC. That certification is earned by completing the NCUTC online curriculum and passing the post-course assessment. The online course discusses radio frequency theory, UAS investigative basics, legal and FAA regulations, and ground intercept teams, among other topics.

Personnel who received an NCUTC Mitigation Certification before July 1, 2026, must complete the online detection and warning curriculum by September 29, 2026. The Mitigation Certification remains valid until then, and the agency's accreditation is not affected while those personnel complete that curriculum.

The two-week course at the NCUTC has a 4:1 student:teacher ratio. The first week features hands-on training with roughly 10 different systems, a current threats briefing, a night detection exercise, and considerations specific to any pending special events. In week two, students work on reconnaissance, system installation, detection and mitigation scenarios, and a realistic offsite protection exercise.

NCUTC will triple throughput in FY 2027 and plans to graduate an additional 300 mitigation operator certificants.

The SAFER SKIES Act

The SAFER SKIES Act, enacted as part of the FY26 NDAA in December 2025, cleared the way for SLTT law enforcement and correctional agencies to handle their own drone mitigation—provided the departments adopt formal policies in line with federal rules and use only certified graduates of the FBI’s NCUTC.⁶³ The federal implementing regulations were issued by DOJ and DHS as an interim rule, published July 6, 2026, but retroactively effective as of July 1, 2026.⁶⁴ (The rule is codified in identical form at 6 CFR part 124 and 28 CFR part 124.)

But the changes produced by the SAFER SKIES Act are dramatic, the main one being that counter-drone mitigation is no longer limited to four federal departments (DOE, DOJ, DoD, and DHS). Before the new federal rules took effect, local SLTT detection and mitigation operations had to be deputized through a federal task force. Under the new framework there is no application to file and no federal approval to wait for. An agency establishes its own accreditation by adopting an implementation policy that satisfies the rule, having agency counsel or a state or local prosecutor review and concur in it, completing the attestation on the federal C-UAS coordination portal, limiting its equipment to the authorized lists, and ensuring its personnel hold the certifications required for the authorities it intends to exercise. Individual operators are certified separately by the NCUTC, which is the sole certifying authority for SLTT C-UAS operators. Accredited agencies report each mitigation action to DOJ and DHS within 48 hours. The framework was open for public comment through September 4, 2026, and could still be revised.

From Interim Rule to Final Rule—What Comes Next

Instead of following the standard rulemaking process—typically lasting 18 to 24 months—DHS and DOJ skipped straight to an interim final rule, which took effect immediately on July 1, 2026. The departments invoked the Administrative Procedure Act’s “good cause” exception, citing Congress’s compressed 180-day statutory deadline and the urgency of securing the FIFA World Cup and America250 events. The rule was legally binding and in effect immediately, but it remained open for public comment through September 4, 2026, and the departments can still revise it based on that feedback before issuing a final rule.

The SAFER SKIES Act also created a civil fine of up to \$100,000 per violation. That fine runs against an SLTT agency, or its personnel, that knowingly takes mitigation action without the federal coordination the law requires, meaning the advance coordination, the real-time air traffic control notification, or the 48-hour post-action notification. It is a penalty on the agency exercising the authority—not on the drone operator. Violations of other requirements of the rule are addressed through the compliance audit program and through suspension of certification

63. The July 1, 2026 Interim Federal Rule codifying a framework for the SAFER SKIES Act also allows the FBI Director to authorize “Federal Law Enforcement Training Centers or another qualified Federal training provider” to provide NCUTC-certified mitigation training.

64. *Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies* (see note 11).

or accreditation. The law also creates a list of authorized technologies jointly maintained by six federal bodies: the DOJ, DHS, DoD, DOT (U.S. Department of Transportation), the FCC, and the National Telecommunications and Information Administration. That framework has two parts: (1) the Authorized Technologies List, which identifies the categories of technology agencies may use, and (2) the Authorized Systems List, which identifies specific makes and models within those categories as they complete interagency assessment.

One issue the SAFER SKIES Act did not fully resolve was later addressed by the FCC. Section 333 of the Communications Act⁶⁵ prohibits willful interference with licensed radio communications—creating potential legal exposure for any SLTT agency that uses RF jamming or signal takeover to mitigate a drone, even with authority under the SAFER SKIES Act. On July 2, 2026, the FCC’s Wireless Telecommunications Bureau issued a declaratory ruling clarifying that mitigation actions validly conducted under the SAFER SKIES Act’s SLTT authority will meet the conditions for Section 333 immunity, removing a legal obstacle that might otherwise have discouraged certified agencies from using RF-based mitigation techniques. Section 333 relief is not the only FCC step, however. An SLTT agency still needs operational authority from the FCC before it operates any C-UAS system that emits RF energy (such as radar), whether that system is used for detection or for mitigation, and that authority is currently granted through a Special Temporary Authority.⁶⁶

Protections for Civil Liberties, Safety, and Trust are Built Into the SAFER SKIES Act.

The SAFER SKIES Act requires that personnel be trained and certified and that their mission be limited in scope and time. Counter-UAS operations must use only authorized technologies, coordinate with the FAA, and avoid any monitoring of content or communications that would violate the First Amendment. Federal oversight of all counter-UAS operations is also required through periodic compliance audits.

The Goal for Future State and Local C-UAS Authorization is a Certification-Based Model.

The new EOs, funding, and statutes point toward a framework that certifies operators, defines operating parameters, and trusts certified agencies to execute independently within those bounds. Operators are required to complete the NCUTC course. Both the individual operator and their agency are then certified by the Attorney General, subject to periodic compliance review audits.

The initial priority for C-UAS authorization was to provide capabilities to jurisdictions hosting the 2026 FIFA World Cup and America250 celebrations. Future funding rounds are expected to build nationwide capacity that could also support preparations for events like the 2028 Summer Olympics.

But special events aren’t the only focus for counter-drone training and authorization. Police organizations from around the country are invited to apply for training at the NCUTC, the crucial first step in gaining authorization for all SLTT police departments.

65. Federal Communications Commission Authorization Act, 47 U.S.C. § 333 (1990), <https://www.govinfo.gov/app/details/USCODE-2024-title47/USCODE-2024-title47-chap5-subchapIII-partI-sec333>.

66. Wireless Telecommunications Bureau, *Application of Section 333 of the Communications Act to Development or Operations of Counter-Unmanned Aircraft Systems for the Federal Government and under the SAFER SKIES Act*, Declaratory Ruling, (Washington, DC: Federal Communications Commission, 2026), <https://www.fcc.gov/document/c-uas-dr-federal-government-and-slts-under-safer-skies-act>.



Photo courtesy Arlington (Texas) Police Department

Eight Things Agencies Can Do Before NCUTC Certification



As of mid-2026, most law enforcement agencies hold only modestly expanded C-UAS authority compared to what they had before the passage of the SAFER SKIES Act in late 2025. The most immediate change is that a pathway to conduct RF-based detection is now open, though the authority is not automatic. Detection using systems that depend on the law, principally RF detection that intercepts or otherwise accesses the drone's command-and-control link, requires four things at the same time:

1. Every person operating the system holds a current Detection and Warning Certification.
2. The agency deploys only systems within a category on the Authorized Technologies List and a specific listed system once the Authorized Systems List is populated for that category.
3. The agency has adopted a detection and warning policy or a full implementation policy, has completed the portal attestation, and has authorized the operation through a written C-UAS Operations Plan.
4. The agency complies with the privacy, data handling, and retention requirements of the rule.

Detection methods that do not depend on the SAFER SKIES Act, including Remote ID reception, cameras, acoustic sensors, and radar operated under FCC authorization, fall outside the rule and remain available on the same basis as before. For most agencies, their authorities are still limited to detecting drone activity and identifying or contacting drone operators. However, agencies do not need to wait for mitigation authority to begin preparing. Departments can take meaningful steps now to strengthen policies, training, interagency coordination, and operational readiness, positioning them to take full advantage of new mitigation authorities once personnel complete the required federal training.

The Detection and Warning Certification is the practical starting point for most agencies. The curriculum is delivered online through the NCUTC training portal at no cost, and the certification issues automatically on successful completion of the course and the post-course assessment. It is also a prerequisite for the resident mitigation course, so an agency that expects to pursue mitigation authority later should begin here now.

Participants in PERF's 2026 meeting consistently emphasized that agencies that begin building partnerships, policies, training plans, and detection capabilities today will be far better positioned to respond when expanded authorities become available.

1. Build Public Support for Counter-UAS Operations

This is listed first because legal authority and technology mean little without the public's support for their use. A department can be fully certified and well equipped, but if residents don't understand or trust why drones are being deployed over their neighborhoods, that authority becomes difficult to exercise in practice—every incident, every complaint, every misunderstanding chips away at the program's legitimacy.

As agencies assume greater responsibilities in the airspace above their communities, residents will likely have questions regarding privacy protections, hobbyist drone activity, data collection, and no-fly zones. Agencies should begin addressing those concerns *proactively*, before new authorities take effect. PERF's 2022 report, *Community Engagement Strategies for State, Local, Tribal, and Territorial Law Enforcement UAS Programs*,⁶⁷ offers several recommendations for police executives.

2. Establish Relationships with the Key Counter-UAS Specific Federal Agencies

The most important step an agency can take today is to establish relationships with federal agencies that already play a role in counter-UAS operations. An agency's local FBI field office should be its primary point of contact for threat reporting, intelligence sharing, training opportunities, special event planning, and future mitigation coordination, but the FAA and FCC also have roles to play.

- **Prepare.**

- Develop a written C-UAS policy that clearly defines roles, responsibilities, legal considerations, and operational procedures.
- Identify candidates for NCUTC training.
- Establish legal relationships and begin incorporating C-UAS scenarios into exercises and training events.

- **Coordinate.**

- Engage with your jurisdiction's FBI field office's C-UAS coordinator as the primary point of contact for deputation, joint operations, intelligence sharing, and investigative support.
- Build relationships the FCC and the FAA to ensure your agency is prepared to operate under future federal mitigation authorities and regulations.

67. PERF (Police Executive Research Forum), *Community Engagement Strategies for State, Local, Tribal, and Territorial (SLTT) Law Enforcement Unmanned Aircraft System (UAS) Programs* (Washington, DC: Office of Community Oriented Policing Services, 2022). <https://www.policeforum.org/assets/DronesCommunityEngagement.pdf>.

- **Report.**
 - Report unauthorized or suspicious UAS activity to your FBI field office.
 - Even seemingly minor incidents can contribute valuable information to regional and national intelligence efforts, helping federal, state, local, tribal, and territorial partners better understand emerging threats and trends.

3. Determine Where the C-UAS Function Will Reside

One of the most important organizational decisions agencies face is determining who will be responsible for counter-UAS operations. Detection technology alone does not create security. The strongest programs are not necessarily those with the most sensors but those with clear ownership of the mission and established procedures for responding when a threat is detected. This step also presents a crucial opportunity to broaden relationships with local partners.

Here are three questions worth answering before you buy a sensor:

1. Who owns the mission?

Should it be housed in a stand-alone unit, the real-time crime center, a fusion center, or a newly created unit? Will it have day-to-day capability or only be maintained for specific events? What command structure and reporting relationships will govern the unit?

2. Who responds when a drone alert is generated?

Will there be a designated ground intercept team, or will patrol personnel be dispatched on an ad hoc basis? What is the expected average response time from alert to operator contacted? Have personnel regularly exercised the full response process—including detection, assessment, communication, deployment, and resolution—or only the detection component?

3. How will information be shared?

Will drone detections be integrated into real-time crime centers, fusion centers, dispatch systems, emergency management operations, aviation units, and neighboring jurisdictions? How will the capability contribute to broader public-safety operations?

4. Plan Ahead for Special Events

For agencies hosting major public events, advance planning remains critical. Until local agencies possess independent mitigation authority, TFRs remain one of the most effective tools available for protecting event airspace.

At present, SLTT agencies seeking FAA-issued drone flight restrictions for large pre-planned events must request a TFR. Eligibility is generally limited to (1) outdoor stadiums or venues that have previously qualified for special security protections and are expected to draw at least 30,000 people or (2) other primarily outdoor events with a defined boundary and an expected attendance of at least 100,000 people.⁶⁸ Once the TFR is obtained, the regional JTTF must be engaged to handle

68. 49 U.S.C. § 44812 Temporary Flight Restrictions for Unmanned Aircraft (2024), <https://www.govinfo.gov/app/details/USCODE-2024-title49/USCODE-2024-title49-subtitleVII-partA-subpartiii-chap448-sec44812>.

mitigation. This process will remain necessary until departments develop and implement federally compliant training, certification, operational procedures, and policies for personnel authorized to conduct mitigation operations under their own authority (following NCUTC certification).

Other suggested steps to prepare for special events include the following:

- Having agency counsel or the jurisdiction’s prosecuting attorney conduct a formal legal review of proposed counter-UAS policies, procedures, and rules
- Establishing relationships and coordination mechanisms with federal partners well before an event occurs
- Coordinating with other local agencies to establish information and resource sharing
- Leveraging funds, personnel, communications, and operational support from local fire departments, airports, and other public sector partners

Cathy Lanier Describes What Chiefs Need to Do to Prepare for the Threat of Malicious Drones

From D.C. police chief to head of NFL security, Cathy Lanier has been grappling for years with the red tape and regulations that limit who can take down a malicious drone. In D.C., Lanier was first introduced to the threat when people flew homemade helicopters over the National Mall and the White House. With the NFL, she had to obtain authorization from the DOJ to take action against drones at the Super Bowl, but the league is not currently authorized to do more than track drones at all other games.



NFL Chief Security Officer Cathy Lanier speaks at PERF’s 2026 meeting

“What we were eventually able to accomplish,” Lanier said in an interview with PERF, “was to simply give state and local law enforcement the same authority that’s already been granted to federal law enforcement. That’s what we’ve been working on for the last five years.”

Here is Lanier’s four-step roadmap for what every department interested in countering malicious drones should begin doing now.

Step one. “You’ve got to take this one-hour [prerequisite to the NCUTC] class [see sidebar on page 29] to understand what ‘detect-track-and-locate’ technology you can and cannot use. Which is an online course, by the way, so that’s easy enough. It is hosted by the FBI, and law enforcement officers have access to it via an online link. Four new documents on the program were sent out in July 2026, describing what is required for the class. Next you have to have a person or a team that goes down to the

5. Assess Critical Infrastructure

Not all drone threats involve major sporting events or public gatherings. Participants at PERF's meeting emphasized their growing concern that critical infrastructure is a potential target for malicious drone activity, because many facilities are difficult to secure from above.

Agencies should comprehensively identify any critical infrastructure that could be targeted by malicious drones. These include energy facilities, data centers, defense bases, ports, transportation hubs, telecommunications infrastructure, and water systems. Beyond identifying these assets, agencies should assess each site's vulnerability to drone incursions; evaluate the potential operational, economic, and public safety consequences of a successful attack; and prioritize facilities based on risk.

FBI's counter-UAS training center in Huntsville, Alabama, that's the team that's trained all of our bomb technicians in the U.S. for the last couple of decades. Your team has to go through that training, it's currently a two-week course."

Lanier said that because a team from the Pennsylvania State Police had been through the training, they were the first state or local team to work with federal authorities on mitigation at the NFL Draft in Pittsburgh in April 2026.

Step two. "You need the equipment. It must be equipment that's authorized by the federal agencies." Lanier cautioned police executives to be wary of vendors soliciting for their business, noting that she had been pitched by countless companies, many of which did not sell authorized equipment.

Step three. "The third piece is policy. So, there are two echelons of policy required: [The first is] the federal interim guidance for state and local law enforcement. While we're waiting on the rule making, the federal government's going to put out an interim guidance that should be out soon. The second policy piece is the state and local law enforcement's internal policy, based off the federal interim guidance. The state and local agency must have their own policy published before they are authorized to use mitigation on their own." [Note: As noted in the sidebar From Interim Rule to Final Rule on page 30, effective July 1, 2026, the federal rule is now in place.]

Step four. "And number four, FCC authorities. The SAFER SKIES Act does not exempt FCC authorities from jamming [radio frequencies] . . . So when you're deploying this equipment, you have to know what your spectrum environment is and the FCC controls that. So you have to coordinate with the FCC."

Lanier added, "Prior to getting to those top four, you want to build your mitigation team. The mitigation team most likely is going to come from your aviation division or your special operations team, right? They've already got pilots' licenses; they know how to operate drones. And you need to start a working group, and that group must include the FCC, the FAA and your federal partners that have been doing this for several years now."

Law enforcement agencies should work with infrastructure operators to develop response protocols; establish points of contact; and identify areas where drone detection, information sharing, or protective measures may be warranted. Leaders should pay particular attention to facilities supporting emergency services, defense operations, energy production and distribution, communications networks, and other functions whose disruption could have cascading effects on public safety and economic stability.

Critical infrastructure owners and operators may also become important partners—not just protected assets—in a jurisdiction’s C-UAS strategy. The 2022 Domestic Counter-UAS National Action Plan—the first federal whole-of-government strategy on this issue—proposed permitting critical infrastructure owners and operators to purchase authorized C-UAS equipment for use by SLTT or federal agencies protecting their facilities.⁶⁹ The FY2026 NDAA’s Section 8602, “Drone Countermeasures to Protect Public Safety and Critical Infrastructure,” offers an early legislative foothold for this kind of arrangement.⁷⁰ Agencies should consider engaging critical infrastructure operators in their jurisdiction now—not only to assess vulnerability but also to explore whether these entities might eventually help fund or maintain shared C-UAS capability.

6. Develop and Implement Lawful Detection Capabilities

Detection remains the area in which most agencies can immediately strengthen preparedness. However, meeting participants repeatedly cautioned agencies to understand the legal and technical implications of any system before acquisition or deployment. Several presenters warned departments not to rely solely on vendor representations regarding their products’ legality or capability. They said agencies often focus first on equipment when they should begin with legal review, policy development, staffing, and training. But a technology purchase that cannot be lawfully deployed—or whose alerts cannot be acted upon operationally—adds little value. Awareness of the system’s functionality and compliance with federal and state laws and regulations are each department’s responsibility. And as criminal prosecutions for drone violations increase, prosecutors should confirm that their agencies’ detection systems operate within the bounds of all wiretap and pen-trap statutes so that evidence derived from those systems will withstand suppression challenges.

With respect to legality, agencies must be aware of FCC and FAA regulations as well as state and federal statutes. FAA Part 107 governs standard Visual-Line-of-Sight drone flights for commercial and recreational drone use, requiring that the pilot or an observer be able to see the drone at all times. Pilots also must pass an FAA test to earn a remote pilot certificate, and drones must weigh less than 55 pounds.

For larger drones, the FAA’s proposed Part 108 would govern Beyond-Visual-Line-of-Sight flights, allowing drones to operate far beyond human sight. Compliance would require operations supervisors and flight coordinators, aircraft certification, and robust detect-and-avoid technology and would apply to drones weighing up to 1,320 pounds. (Part 108 remains a proposed rule as of this writing and is not yet final. Readers should verify its status and any requirements directly through the Federal Register or FAA rulemaking resources.

69. “FACT SHEET: The Domestic Counter-Unmanned Aircraft Systems National Action Plan,” The White House, last modified April 25, 2022, <https://bidenwhitehouse.archives.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/>.

70. National Defense Authorization Act for Fiscal Year 2026 (see note 23).

In 2020, an Interagency Legal Advisory issued jointly by DOJ, DOT, FCC, and DHS strongly recommended that, prior to the testing, acquisition, installation, or use of any C-UAS system, entities seek the advice of counsel experienced with both federal and state criminal, surveillance, and communications laws.

Beyond legality, a department should fully understand a system's actual functionality. It must know what data it captures; comply with the data collection, retention, and dissemination requirements in the interim rule (see sidebar, page 30); and understand how it interacts with the National Airspace System.

Current Forms of Legal Detection

Although mitigation authority remains limited, agencies have several lawful options for detecting and locating drones. These include the following:

- Remote ID broadcast reception, in which a drone's identifying beacon is used to identify the owner and the owner's location so police can find the operator and redirect the drone
- Electro-optical or infrared cameras, which can spot drones and alert law enforcement
- Acoustic sensors, which can detect the sounds of drones and alert police
- Radar systems and RF energy measurement tools, which can also detect the presence of drones that might otherwise be missed by standard observational measures

Each technology has strengths and limitations, and agencies should evaluate systems based on operational requirements rather than marketing claims.

In turn, a department must be aware of the implications of a system's interactions with the FCC, including its recent decisions (see note 66), the FAA, and the regional radio spectrum. Radar-based systems require FCC licensing. Some systems' emissions may interfere with other, established radio frequencies.

Any system that, in detection mode, captures or decodes drone-to-controller communications or intercepts electronic communications requires personnel who hold a current Detection and Warning Certification from the NCUTC, equipment drawn from the authorized lists, and an accredited agency operating under an adopted policy and a written operations plan. Mitigation of drones through cyber-based takeover or disruption, RF jamming, seizure or forced landing, kinetic defeat by shooting down or capturing a drone, or GPS spoofing remains solely under federal authority for any given department until its personnel hold a Mitigation Certification and the department is accredited under the interim rule. These are separate steps, and an agency may pursue detection and warning authority without pursuing mitigation authority at all.

UAS Incident Reporting Checklist

The questions below are designed to capture the critical information needed to assess, investigate, and respond to a suspected UAS incident. Include as much detail as possible and attach supporting documentation when available.

- What was the reporting party's location when the suspected UAS was observed? Record the location using geographic coordinates or, if available, a map application.
- What were the start and end times of the suspected sighting of the UAS (specific date, time, and time zone)?
- Was the suspected UAS assessed against alternative explanations (for example, aircraft, satellites, celestial objects, or other aerial phenomena) using flight-tracking or astronomy applications, if available?
- If the UAS operator(s) were observed and/or interviewed what information, including any biographic information, was obtained?
- Note the location of the UAS operator in relation to the DoD/DCI facility, indicating details such as the range of the UAS, operator line of sight, and view of any sensitive facility equities.
- Was the UAS visually or audibly detected? Please attach any photos and/or videos of the UAS to the report, if available.
- What was the direction and bearing of the UAS (for example, North or South)? Did the UAS move, hover, or fly fast in one direction?
- What type of UAS was observed—fixed-wing, multi-rotor, rotary-wing, hybrid, or unknown?
- Were there any TFRs or flight restrictions in place at the time and location of the incident? If so, attach a copy of the restrictions.
- What other details were observed (for example, the color or pattern of lights, number and location of lights, path or movement behavior)? If anything was attached to the UAS, what did the attachment look like (i.e., did it resemble a sprayer, antennas, small rocket, weapon, or box)?
- If anything fell, launched, or released from the UAS, what was the altitude, and where in the path of movement was the item released? If the released item was recovered, which agency currently possesses it?
- What type of UAS detection system exists at your site, if any? Did the system detect the UAS? If so, what data were collected (for example, telemetry, flight path information, or .xml files)? Please include whether the system collected any information from the UAS, including .xml files or movement paths.
- For those with C-UAS Authority and Capability: If a UAS mitigation system was used, what is the system name, time/duration used, and outcome? Where was the UAS operator located when it was used? In what direction was the system pointed during use?

Source: This guidance is a slightly modified version of the reporting guidance provided in Office of the Private Sector, Unmanned System Incursions of DoD Installations and Defense Critical Infrastructure Sites, S-241028-012 (Washington, DC: Federal Bureau of Investigation, n.d.).

7. Report Every Significant Drone Incident

Federal authorities urged agencies to consistently report suspicious or unauthorized drone activity through FBI channels and the eGuardian system. Even incidents that appear isolated may contribute to broader intelligence efforts when combined with reporting from other jurisdictions.

The NJTTF reported at the 2026 PERF meeting that eGuardian had received 1,385 total reports during the 10-month period from June 2025 to April 2026. Investigations into the reports resulted in the closure of 1,270 cases; 115 are still being processed.

8. Pursue NCUTC Training and Agency Accreditation

As noted in the sidebar on page 29, NCUTC certification is the linchpin to obtaining C-UAS authority, but the two certifications sit at different points in the process. The Detection and Warning Certification comes first. It is delivered online at no cost and requires no nomination and no travel; an agency can begin it immediately. Paired with an adopted implementation policy, legal review and concurrence, and the portal attestation, it establishes the agency accreditation that authorizes detection and warning operations. Agencies that then decide to pursue mitigation need the resident NCUTC course, and for that they should contact their local FBI field office, which is the point of contact for nominations. The FBI centrally reviews and prioritizes seats based on operational need and jurisdictional responsibility rather than on funding source or the order of requests.⁷¹ General inquiries can be directed to ncutc@fbi.gov.⁷² Given the volume of interest driven by the 2026 World Cup and America250 preparation, agencies should plan lead time rather than assuming a seat will be available on request. NCUTC is tripling its throughput and projects roughly 400 graduates by the end of fiscal year 2027, but receiving C-UAS grant funding does not by itself guarantee a training seat.

71. Jim Magill, “Training for the Threat: FBI Expands Counter-UAS Training Ahead of Historic World Cup,” DroneLife, last modified February 17, 2026, <https://dronelife.com/2026/02/17/fbi-counter-uas-training-world-cup-2026/>.

72. FBI (Federal Bureau of Investigation), “Announcement of the NCUTC and Initial Training,” memorandum to all U.S. law enforcement agencies, September 24, 2025, <https://iaclea.org/wp-content/uploads/2025/12/NCUTC-Announcement-Memo.pdf>.

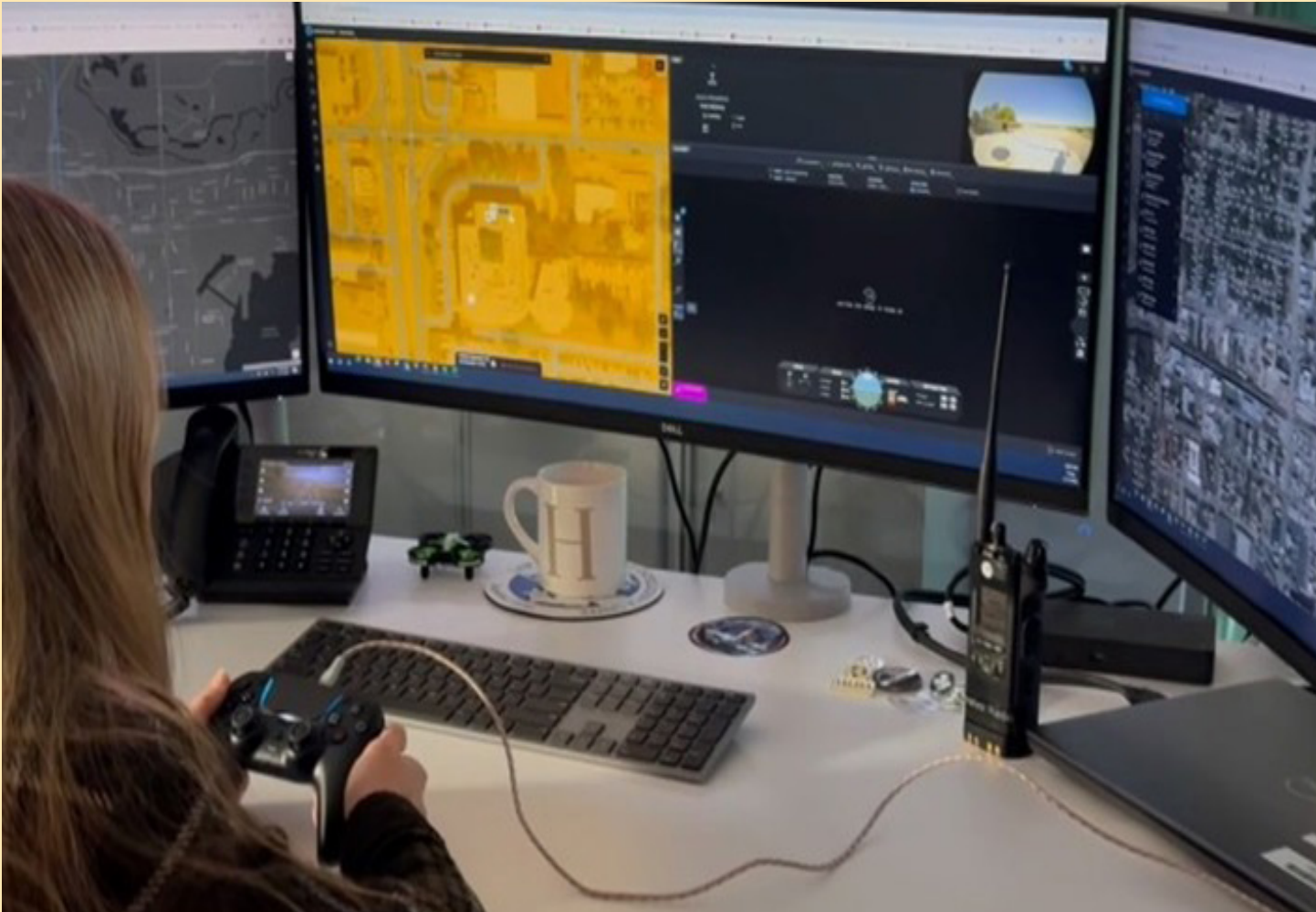


Photo courtesy Arlington (Texas) Police Department

After Certification— Four Ways to Build a Sustainable C-UAS Capability



NCUTC certification is a starting point, not a finish line. If an agency has personnel who obtained NCUTC certification before the SAFER SKIES Act’s interim implementing rule took effect on July 1, 2026, those individuals operated under federal task force deputation until that date as a temporary measure. Meanwhile, the NCUTC’s main priority was training local police in the 11 World Cup cities—though other departments could pursue certification as well—as a first step toward drone mitigation ahead of the interim rule’s effective date.

But that deputation was always intended as a bridge. Now that the interim rule is in effect, agencies pursuing mitigation authority should move toward independent, agency-level certification—training more personnel through NCUTC, limiting equipment to the jointly authorized systems list, and complying with the rule’s reporting requirements—rather than relying on federal task force deputation alone. Deputization may still apply to certificants operating under earlier arrangements or departments awaiting full agency-level certification.

Building a program that can sustain long-term independence requires more than certification alone. Based on discussions at PERF’s 2026 meeting, four steps stand out:

1. Move Toward Independent Operations

Federal task force deputation was never meant to be a permanent solution. As FBI Assistant Section Chief Torphy said at PERF’s meeting, relying on federal deputization—and engaging the FBI in individual operations one at a time—is “impractical for the bureau.” That model, he noted, was only sustainable for defined campaigns, not for permanent daily operations nationwide, and continued reliance on deputation would defeat the purpose of the mitigation authority Congress granted to SLTT law enforcement in the first place.

The move to independent operations means the agency, and not just individual deputized officers, holds mitigation authority. The requirements are as follows:⁷³

- Agency accreditation, established through policy adoption, legal review and concurrence, and portal attestation, in addition to individual NCUTC certification
- Equipment limited to the Authorized Technologies List and to the Authorized Systems List where that list has been populated for a particular category, both jointly maintained by DOJ, DHS, DoD, DOT, the FCC, and NTIA
- A current Mitigation Certification for every person executing a mitigation action, plus a current FAA part 107 remote pilot certificate
- A written C-UAS Operations Plan authorizing the operation
- Advance airspace and spectrum coordination and real-time air traffic control notification
- A credible threat determination; SLTT mitigation authority reaches credible threats to the safety or security of people, facilities, and assets; a venue or set of venues used for large-scale public gatherings or events; critical infrastructure; or a correctional facility
- Notification to DOJ and DHS within 48 hours of every mitigation action

For most agencies, this transition will be gradual, with some personnel certified as others remain in training. The federal relationship built during deputation does not end—it shifts from *needing* federal authority to act to *exercising authority independently*, with federal partners available to coordinate and support.

2. Develop Internal Policy and Oversight

Federal certification determines whether an agency may exercise mitigation authority; internal policy determines how it will do so. As NFL Chief Security Officer Cathy Lanier explained earlier in this report (sidebar on page 36–37), agencies must layer their own policy on top of federal guidance before they are authorized to act—and that policy must be designed to function after certification, not merely to satisfy it once.

That means clear rules on when mitigation is used, who can authorize it, and how it's documented—paired with after-action review of every mitigation event, not just those that go wrong. Oversight should extend to the compliance audits required under the final rule and connect back to the public-trust work described earlier in this chapter: Agencies that can show they use mitigation authority consistently and transparently will have an easier time maintaining community support than those that treat oversight as a paperwork requirement.

73. *Counter-UAS Authority for State, Local, Tribal, and Territorial Law Enforcement and Correctional Agencies* (see note 11).

3. Integrate C-UAS into Existing Operations

Detection and mitigation authority is of minimal value when siloed. The question raised earlier in this report—Where should the C-UAS function live within a department? (see page 35)—becomes operational once an agency is certified: Alerts have to reach whichever location the agency chooses, whether an RTCC, a fusion center, or a stand-alone unit. And the people authorized to act on those alerts need to be embedded in that structure, not waiting on a separate channel.

Some agencies are already integrating across jurisdictional lines. In Michigan, for example, university and state police created a statewide drone association that integrates detection data from roughly 32 agencies through a single third-party vendor—regardless of which detection software each agency uses individually (see sidebar *Securing America's Stadiums* on page 24–25). The association is also developing a historical search function that allows agencies to trace a drone's prior activity across jurisdictions by serial number.

4. Build Sustained Proficiency

Like any perishable tactical skill, mitigation readiness degrades without regular practice; agencies should build recurring scenario-based exercises into their training calendar rather than relying solely on the initial NCUTC course.

Sustained proficiency also depends on not only establishing but also maintaining coordination with the FCC and FAA. Spectrum environments and airspace considerations can shift with new construction, new events, or new deployments nearby; a working relationship built once during onboarding needs to stay active.



Photo courtesy Longmont (Colorado) Police Department



Conclusion

Drone technology has evolved far faster than the policies, authorities, and capabilities designed to address its misuse. Since PERF first sounded the alarm about the threat of malicious drones in 2019, UAS have become cheaper, more capable, more autonomous, and more widely available. Around the world, criminals, cartels, terrorists, and nation-states have demonstrated how drones can be used to surveil targets, disrupt operations, attack critical infrastructure, and inflict harm with little cost and minimal risk to the operator. Meanwhile, unauthorized drone activity has become a routine challenge for law enforcement agencies responsible for protecting major events, public gatherings, correctional facilities, and critical infrastructure.

As of this writing, the United States has been spared a catastrophic malicious drone attack. But participants at PERF's 2026 meeting repeatedly cautioned that the absence of such an incident should not be mistaken for the absence of risk. Rather, it should be viewed as an opportunity to prepare before a major event forces change through tragedy.

For years, law enforcement agencies have faced a frustrating reality: They could often detect a suspicious drone but lacked the authority or tools necessary to intervene. That gap between responsibility and capability has been one of the central challenges discussed in PERF's drone-related work over the last seven years.

That gap is beginning to close.

The SAFER SKIES Act, the establishment of the FBI's NCUTC in Alabama, new federal grant funding, and recent executive actions collectively represent the most significant expansion of state and local counter-drone capability in U.S. history. For the first time, a pathway exists for properly trained and certified law enforcement agencies to develop their own counter-UAS capabilities within a framework designed to protect public safety, civil liberties, and the national airspace.

But this report's central message is not about legislation, funding, or technology. It is about preparedness. Successful agencies will

- recognize that malicious drone activity is no longer a future concern but a current and growing public safety challenge;
- take advantage of emerging authorities, funding opportunities, and training programs to build sustainable counter-UAS capabilities;
- invest in policies, legal review, training, and interagency partnerships before a crisis occurs;
- build public trust through transparency, oversight, and clear safeguards governing counter-drone operations;
- view counter-UAS capability as an essential component of modern public safety rather than a niche function reserved for major events.

Effective counter-UAS programs will not be built overnight, nor will they be built through equipment purchases alone. Leadership, planning, community trust, and sustained investment will ultimately determine whether agencies are prepared to meet this evolving threat.

The question facing police leaders is no longer whether drones will become a significant public safety issue. That question has already been answered. The question now is whether law enforcement agencies will be prepared to respond to a threat that is increasingly common, sophisticated, and capable of affecting the communities they serve. Twenty-five years after the 9/11 Commission cited a “failure of imagination” as one of the root causes of the catastrophic loss of life on September 11, 2001, the question is whether agencies will heed the warnings already in front of them or wait for a similar failure to repeat itself with drones.

Agencies that succeed will be those that act before a major incident occurs, not after. The time to prepare is now.



Appendix A. Glossary

ASL	authorized systems list
ATL	authorized technologies list
BVLOS	beyond visual line of sight
C-UAS	counter–unmanned aircraft system (counter-drone)
C-UAV	counter–unmanned aerial vehicle (counter-drone)
DJI	leading manufacturer of commercial drones; importantly, DJI is a Chinese-owned company, which has led to national security concerns and an effective U.S. ban on new DJI products
DOD	U.S. Department of Defense (a.k.a. Department of War)
DOW	U.S. Department of War (a.k.a. Department of Defense)
eGuardian	FBI’s system for reporting unauthorized drones
EO 14305	Executive Order titled <i>Restoring American Airspace Sovereignty</i> , focused on accelerating counter-drone capabilities to protect public safety and critical infrastructure; issued on June 6, 2025
EO 14307	Executive Order titled <i>Unleashing American Drone Dominance</i> , focused on expanding remote drone operation, integrating U.S.-manufactured drones into the national airspace system, and combining AI with drones; issued on June 6, 2025
FEMA	Federal Emergency Management Agency

FIFA	Federation Internationale de Football Association (International Federation of Association Football)
JTTF	Joint Terrorism Task Force
NCUTC	National Counter-UAS Training Center, the FBI’s counter-drone training facility in Redstone Arsenal, Alabama
NDAA	National Defense Authorization Act
NJTTF	National Joint Terrorism Task Force
NOFO	notice of funding opportunity
OBBA Act	One Big Beautiful Bill Act; among many other things, this provides grant funding for C-UAS related capabilities for state and local law enforcement; signed into law on July 4, 2025
RF	radio frequency
RTCC	real-time crime center, also often called a “real-time <i>information</i> center” or “real-time <i>intelligence</i> center.”
SAFER SKIES Act	federal legislation enacted in December 2025 that extended counter-UAS detection, warning, and mitigation authority to certified SLTT law enforcement and correctional agencies; codified at 6 USC §124n
SLTT	state, local, tribal, and territorial
SOP	standard operating procedure
sUAS	small unmanned aircraft system (drone)
sUAV	small unmanned aerial vehicle (drone)
sUUV	small unmanned underwater vehicle/vessel (drone)
TFR	temporary flight restriction
UAE	United Arab Emirates
UAS	unmanned aircraft system (drone)
UAV	unmanned aerial vehicle (drone)
UUV	unmanned underwater vehicle/vessel (drone)
VLOS	visual line of sight
VTOL	vertical takeoff and landing

Appendix B. Resources



The SAFER SKIES Act

The SAFER SKIES Act, passed as part of the National Defense Authorization Act (NDAA) in December 2025, for the first time authorized state, local, tribal, and territorial police to conduct their own counter-drone mitigation—provided the departments create their own formal policy guidance in line with federal rules and use certified graduates of the FBI’s national training center. The implementing regulations were issued jointly by DOJ and DHS as an interim rule, effective July 1, 2026, and published in the Federal Register on July 6, 2026, codified in identical form in 6 CFR part 124 and 28 CFR part 124. The public comment period closed September 4, 2026.

The relevant law amends 6 U.S.C. § 124n. It is described as intending “[t]o expand the authority to use counter-unmanned aircraft system technologies to state, local, tribal and territorial law enforcement and correctional agencies, and for other purposes.”

SAFER SKIES Act, Division H, Title LXXXVI of the National Defense Authorization Act for Fiscal Year 2026, Pub. L. No. 119–60, §§ 8601–8607, 139 Stat. 718, 1938–1945 (2025) (codified as amended at 6 U.S.C. § 124n) (protection of certain nuclear facilities and assets from unmanned aircraft), <https://www.govinfo.gov/app/details/PLAW-119publ60/related>.

Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks (2020)

A clear call to action on counter-drone preparedness, highlighting gaps in local authority and technology. This was the go-to report on how police use drones—and it warns of the emerging risk of malicious and terrorist drone threats. It synthesizes surveys, interviews, and a national conference to document promising practices, legal constraints, and operational lessons.

PERF (Police Executive Research Forum), Drones: A Report on the Use of Drones by Public Safety Agencies—and a Wake-Up Call about the Threat of Malicious Drone Attacks (Washington, DC: Office of Community Oriented Policing Services, 2020), <https://www.policeforum.org/assets/Drones.pdf>.

Roadmap to Implementing an Effective Unmanned Aircraft System (UAS) Program (2020)

A concise, implementation-focused playbook “by the field, for the field.” This report provides a practical, eight-step, start-to-finish guide for agencies launching or formalizing drone programs. It translates law, policy, training, staffing, and procurement issues into field-ready decision points.

Lisa Mantel, Roadmap to Implementing an Effective UAS Program (Washington, DC: Office of Community Oriented Policing Services, 2020), <https://www.policeforum.org/assets/UASRoadmap.pdf>.

Community Engagement Strategies for State, Local, Tribal, and Territorial Law Enforcement Unmanned Aircraft System Programs (2022)

Shifts the conversation from technology to legitimacy, privacy, and sustained community support. This publication focuses exclusively on building public trust around police drone use through transparency and engagement. It offers concrete outreach tools—web content, presentations, demonstrations, and sample messaging.

PERF (Police Executive Research Forum), Community Engagement Strategies for State, Local, Tribal, and Territorial (SLTT) Law Enforcement Unmanned Aircraft System (UAS) Programs (Washington, DC: Office of Community Oriented Policing Services, 2022). <https://www.policeforum.org/assets/DronesCommunityEngagement.pdf>.

Unmanned Aircraft Systems (UAS): Evolving Risks to Large-Scale Public Gatherings (April 2026)

This white paper reviews the UAS risk landscape; tactics, techniques, and procedures (TTP); and security planning considerations for major events with specific focus on the FIFA World Cup 2026. It was produced as a collaboration between the Center for Internet Security (CIS) and DroneSec, with review and input from the Major County Sheriffs of America (MCSA), the Major Cities Chiefs Association (MCCA), the Association of Law Enforcement Intelligence Units (LEIU), the Small and Rural Law Enforcement Executives Association (SRLEEA), the National Center for Spectator Sports Safety and Security (NCS4), the New Jersey State Police (NJSP), the Institute for Strategic Dialogue (ISD), DRONERESPONDERS, and Aerisq Solutions.

Center for Internet Security, Unmanned Aircraft Systems (UAS): Evolving Risks to Large-Scale Public Gatherings (Clifton Park, NY: Center for Internet Security, 2026), <https://www.cisecurity.org/insights/white-papers/uas-evolving-risks-to-large-scale-public-gatherings>.

Designation-Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility

This action would implement section 2209 of the FAA Extension, Safety and Security Act of 2016 by establishing a process for operators and proprietors of certain fixed site facilities to request and maintain an unmanned aircraft flight restriction (UAFR). The proposal also establishes requirements for applicants to demonstrate the UAFR is necessary for aviation safety, protection of people and property on the ground, national security, or homeland security. Lastly, the proposal identifies the types of operations that are allowed in the UAFR area. Comments were initially due on or before July 6, 2026; on June 30, the comment period was extended to August 5, 2026.

FAA (Federal Aviation Administration), Designation-Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility, 91 Fed. Reg. 24650 (May 6, 2026), <https://www.govinfo.gov/app/details/FR-2026-05-06/2026-08943>; FAA, Designation-Restrict the Operation of Unmanned Aircraft in Close Proximity to a Fixed Site Facility; Extension of Comment Period, 91 Fed. Reg. 39568 (June 30, 2026), <https://www.govinfo.gov/app/details/FR-2026-06-30/2026-13126>.

Interagency Legal Advisory (2020)

Advisory on the application of federal laws to the acquisition and use of technology to detect and mitigate UAS. This is the starting point for any agency considering C-UAS technology acquisition.

FAA (Federal Aviation Administration), (DOJ) Department of Justice, (DHS) Department of Homeland Security, and (FCC) Federal Communications Commission. Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems, August 17, 2020. <https://docs.fcc.gov/public/attachments/DOC-366222A1.pdf>.

DHS/FEMA C-UAS Grant Program

Notice of Funding Opportunity (NOFO) for SLTT law enforcement C-UAS capability development.

DHS (Department of Homeland Security), FEMA (Federal Emergency Management Agency). Counter-Unmanned Aircraft Systems (C-UAS) Grant Program Notice of Funding Opportunity (NOFO), Fiscal Year 2026. October 28, 2025.
https://www.fema.gov/sites/default/files/documents/fema_gpd_fy26_cuas-nofo.pdf.

NCUTC: National Counter-UAS Training Center

The National Counter-UAS Training Center (NCUTC) is the sole certifying authority for SLTT C-UAS operators under the SAFER SKIES Act.

Contact the NCUTC at ncutc@fbi.gov; you can find the NCUTC website on the FBI LEEP JusticeConnect portal via <https://le.fbi.gov/informational-tools/leep>.

Your Local FBI Field Office

The C-UAS coordinator at your local FBI Field Office is your primary coordination channel for UAS threat reporting and partnership.

The FBI's official directory of its 56 field offices across the U.S. and Puerto Rico, listing addresses, phone numbers, and the counties or regions each office covers. The starting point for identifying and contacting an agency's local FBI field office and its C-UAS coordinator.

FBI (Federal Bureau of Investigation). Field Offices, Accessed July 2026.
<https://www.fbi.gov/contact-us/field-offices>.

The Police Executive Research Forum

The **Police Executive Research Forum (PERF)** is an independent think tank and research organization that focuses on critical issues in policing. Since its founding in 1976, PERF has identified best practices on fundamental issues such as reducing police use of force; developing community policing and problem-oriented policing; using technologies to deliver police services to the community; and developing and assessing crime reduction strategies. Over the past decade, PERF has led efforts to reduce police use of force through its *Guiding Principles on Use of Force*⁷⁴ and Integrating Communications, Assessment, and Tactics (ICAT) training program.⁷⁵

PERF strives to advance professionalism in policing and to improve the delivery of police services through the exercise of strong national leadership; public debate of police and criminal justice issues; and research and policy development. The nature of PERF's work can be seen in the reports PERF has published over the years. Most of these reports are available without charge online.⁷⁶ All the titles in the *Critical Issues in Policing* series can be found on the PERF website.⁷⁷ Recent reports include *Managing Officer-Involved Critical Incidents: Guidelines to Achieve*

-
- 74. PERF, *Guiding Principles on Use of Force*, Critical Issues in Policing (Washington, DC: Police Executive Research Forum, 2016), <https://www.policeforum.org/assets/guidingprinciples1.pdf>.
 - 75. PERF, "ICAT: Integrating Communications, Assessment, and Tactics," accessed February 13, 2025, <https://www.policeforum.org/icat>.
 - 76. PERF, "PERF Reports," accessed February 13, 2025, <http://www.policeforum.org/free-online-documents>.
 - 77. PERF, "Critical Issues in Policing Series," accessed February 13, 2025, <https://www.policeforum.org/critical-issues-series>.

Consistency, Transparency, and Fairness,⁷⁸ *The First Six Months: A Police Chief's Guide to Starting Off on the Right Foot*,⁷⁹ and *Embracing Civilianization: Integrating Professional Staff to Advance Modern Policing*.⁸⁰

In addition to conducting research and publishing reports on our findings, PERF conducts management studies of individual law enforcement agencies; educates hundreds of police officials each year at the Senior Management Institute for Police,⁸¹ a three-week executive development program; and provides executive search services to governments looking to conduct national searches for their next police chief.

All PERF's work benefits from its status as a membership organization of police officials and its access to police executives, who share information and open their agencies to research and study. PERF members also include academics, federal government leaders, and others with an interest in policing and criminal justice.

All PERF members must have a four-year college degree and subscribe to a set of founding principles, emphasizing the importance of research and public debate in policing, adherence to the Constitution and the highest standards of ethics and integrity, and accountability to the communities that police agencies serve.

PERF is governed by a member-elected President and Board of Directors and a Board-appointed Executive Director.



78. PERF, *Managing Officer-Involved Critical Incidents*, Critical Issues in Policing (Washington, DC: Police Executive Research Forum, 2025), <https://www.policeforum.org/assets/ManagingOICIs.pdf>.

79. PERF, *The First Six Months*, Critical Issues in Policing (Washington, DC: Police Executive Research Forum, 2025), <https://www.policeforum.org/assets/FirstSixMonths.pdf>.

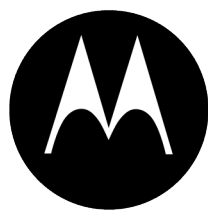
80. PERF, *Embracing Civilianization*, Critical Issues in Policing (Washington, DC: Police Executive Research Forum, 2024), <https://www.policeforum.org/assets/Civilianization.pdf>.

81. PERF, "Preparing Police Executives for the Challenges of Today and Tomorrow," accessed November 25, 2025, <https://www.policeforum.org/smip>.

The Motorola Solutions Foundation

As the charitable and philanthropic arm of Motorola Solutions, the Motorola Solutions Foundation partners with organizations around the world to build safer cities and thriving communities. We focus on giving back through strategic grants, employee volunteerism, and other community investment initiatives. Our strategic grants program supports organizations that offer first responder programming and technology and engineering education, and align to our values of accountability, innovation, impact, and inclusion.

For more information on the Foundation, visit www.motorolasolutions.com/foundation.



Motorola Solutions
Foundation

Critical Issues in Policing

Strengthening Justice: Strategies for Effective Prosecutor-Police Partnerships

Opioid Deaths Fall as Law Enforcement and Public Health Find Common Ground

The First Six Months: A Police Chief's Guide to Starting Off on the Right Foot

Call for Help: Treatment Centers for Police Officers

Managing Officer-Involved Critical Incidents: Guidelines to Achieve Consistency, Transparency, and Fairness

The Carjacking Crisis: Identifying Causes and Response Strategies

Embracing Civilianization: Integrating Professional Staff to Advance Modern Policing

Rethinking the Police Response to Mental Health-Related Calls: Promising Models

Responding to the Staffing Crisis: Innovations in Recruitment and Retention

Building Public Trust Podcast

Women in Police Leadership: 10 Action Items for Advancing Women and Strengthening Policing

Transforming Police Recruit Training: 40 Guiding Principles

Police Chiefs Compensation and Career Pathways: PERF's 2021 Survey

Rethinking the Police Response to Mass Demonstrations: 9 Recommendations

Lessons Learned from the COVID-19 Pandemic: What Police Learned from One of the Most Challenging Periods of Our Lives

An Occupational Risk: What Every Police Agency Should Do To Prevent Suicide Among Its Officers

Chapter 2: How Police Chiefs and Sheriffs Are Finding Meaning and Purpose In the Next Stage of Their Careers

ICAT: Integrating Communications, Assessment, and Tactics

Guiding Principles on Use of Force

Re-Engineering Training on Police Use of Force

An Integrated Approach to De-Escalation and Minimizing Use of Force

Strategies for Resolving Conflict and Minimizing Use of Force

Chief Concerns: Exploring the Challenges of Police Use of Force

To see the full Critical Issues series, visit www.policeforum.org/critical-issues-series.



Police Executive Research Forum
1120 Connecticut Avenue, NW, Suite 930
Washington, DC 20036
202-466-7820
www.PoliceForum.org

We are grateful to the
Motorola Solutions
Foundation for its
support of the Critical
Issues in Policing Series



Motorola Solutions
Foundation