



# WIDENING THE APERTURE PART II: INSTALLATION— COMMUNITY COOPERATION AGAINST DRONE THREATS

APRIL 2026



## ACKNOWLEDGEMENTS

---

### Authors

**Peter Keiser**, Matrix Design Group

**Sal Nodjomian**, Matrix Design Group

**Brad Johnson**, Matrix Design Group

**Charlie Perham**, Matrix Design Group

**Eric Turner**, Matrix Design Group

### Editor

**Randy Ford**, Association of Defense Communities

### Layout

**Charles Watson**, Association of Defense Communities

## CREDITS

---

Front Cover: Photo by Cpl. Joshua Barker

Page 3: Photo by Spc. Nicole Miller

Page 4: Photo by Bobby Cummings

Page 7: Photo by Pfc. Peter Bannister

Page 8: Photo by Spc. Rebeca Soria

Page 9: Photo by Becki Bryant

Page 10: Photo by Spc. Prince Joshua Igbokwe

*The appearance of U.S. Department of War visual information does not imply or constitute DOW endorsement.*

# CONTENTS

---

Acknowledgements .....	2
Credits .....	2
Introduction .....	4
The Nature of the Threat .....	5
The Critical Question: How to Enable Effective Response? .....	6
When Authorities Collide .....	9
Solutions: What Does Success Look Like? .....	10
A Note on Resourcing .....	13
Conclusion .....	14



## INTRODUCTION

On January 12, 2026, Brigadier General Matt Ross, Director of the Department of War's leading entity for countering small Unmanned Aircraft Systems (UAS), stated<sup>1</sup>, "Drones are a defining threat for our time. Technology is evolving fast and our policies and c-UAS strategy must adapt to meet this reality. Countering drones does not start and stop at the fence line."

This statement is one of hundreds of similar statements made by U.S. policymakers and executives, all highlighting the enormous impact that unmanned systems have made in defense policymaking and recognizing the unique threat drones pose to our military installations and their partner communities. As discussed in the first article in this series, *Defining the Threat*, drones represent an emergent threat that deserve to be in this spotlight. We define an emergent threat as one that contains "emergent" technology that has recently reached the point of affecting the landscape of modern warfare and national security. Specifically, emergent threats carry serious ramifications for our military installations and the shared military-civilian infrastructure on which our service members and defense communities depend.

This article provides an in-depth, unclassified discussion of the emergent drone threat and the shared challenges it presents to defense communities and their partner military installations. This discussion begins with an explanation of the nature of drone threats and the reason that they are considered emergent threats of high importance in defense-related contexts. The next section provides a brief analysis of relevant U.S. defense and homeland security policy followed by an examination of what actions are currently being taken to build common ground between defense communities and military installations against drone threats. Finally, we close by exploring possible pathways for installation–community partnerships to meet their shared drone-related challenges.

Emergent threats including those from drones won't be solved by installation–community partnerships alone. Combating these threats requires innovative actions that can be tailored to the unique circumstances of individual military installations and coordinated with relevant military and federal entities. As this article discusses, these are exactly the kind of actions that defense communities and their partnerships can deliver in coordination with military and federal authorities.



<sup>1</sup> JIATF-401 Announces Updated Guidance to Counter Drone Threats in the Homeland. (2026). U.S. Department of War. <https://www.war.gov/News/Releases/Release/Article/4389392/jiatf-401-announces-updated-guidance-to-counter-drone-threats-in-the-homeland/>.

# THE NATURE OF THE THREAT

## Key Takeaways

- United States installations and critical interdependencies (utilities, commodities, etc.) with defense communities are at risk from small commercial drones that can be repurposed as weapons at relatively low cost.
- Unauthorized drone incursions at U.S. military installations and near critical shared infrastructure have risen in recent years while the U.S. military seeks options to detect, deter, and respond to drone threats.

As the first article in this series describes, various government and scholarly sources use the terms “unmanned systems” or “unmanned aircraft systems” as interchangeable labels for drones. However, this analysis uses the term “drone,” since it is the most recognizable and because most people will picture a small, multi-rotor, commercial-style drone when that term is used. These small commercial drones best represent the emergent threat.

This may seem counterintuitive at first glance. Many other systems such as the Iranian-made Shahed or the American-made Reaper can carry more destructive payloads over longer distances and are purpose-built for military applications. However, those larger drone types are specifically designed for employment on a conventional battlefield and provide more challenges to conventional military tactics as opposed to homeland defense in the Continental United States. Small drones, classified by the Federal Aviation Administration’s (FAA) standard of weighing less than 55 lbs.<sup>2</sup> at takeoff, are more dangerous to U.S. installations and their defense community partners precisely because they are:

- Readily available commercially,
- Simple to operate,

- Easy to modify for destructive purposes, and
- Difficult to identify as a threat in real time.

These characteristics, especially when combined, make these drones a potentially ideal tool for sabotage, surveillance, or terror attacks on American soil.

Two widely publicized recent events provide perfect case studies in how these drones can be used by a small number of infiltrators to conduct strategic attacks on military-related infrastructure. The events are Ukraine’s “Spider’s Web”<sup>3</sup> attack on Russian air bases, which destroyed or severely damaged numerous nuclear-capable Russian Air Force bombers in four separate locations hundreds of miles inside Russia, and Israel’s “Operation Rising Lion,”<sup>4</sup> which was a massively complex attack on a host of Iranian air defense and command and control systems effected as a prelude to Israel’s more conventional air offensive against Iran. The specific details of these operations have been discussed in other venues and publications at length, but it is worth noting a few similarities between them for the purposes of this analysis:

- Both attacks were vastly successful, achieved virtually complete surprise, and caused direct damage to high-value targets.
- Both attacks required extensive planning by highly capable military organizations and involved the preparation and staging of materials and personnel across international borders.
- Both attacks utilized commercial logistics and publicly available services from providers in the enemy nation that had no idea they were assisting in an attack on their home soil.
- Both attacks caused billions of dollars in damage by attaching relatively small yields of explosives to commercially purchased and modified drones.
- Both attacks utilized relatively few operators controlling multiple drones or “swarms,” a lower than one-to-one allocation of operator-to-system or operator-to-target.

2 FAA. (2020, October 6). Small Unmanned Aircraft Systems (UAS) Regulations (Part 107) | Federal Aviation Administration. Faa.gov. <https://www.faa.gov/newsroom/small-unmanned-aircraft-systems-uas-regulations-part-107>.

3 Dahlgren, M., & MacKenzie, L. (2025, June 4). Ukraine’s Drone Swarms Are Destroying Russian Nuclear Bombers. What Happens Now? Csis.org. <https://www.csis.org/analysis/ukraines-drone-swarms-are-destroying-russian-nuclear-bombers-what-happens-now>.

4 Walla, K. (2025, June 14). By fusing intelligence and special operations, Israel’s strikes on Iran are a lesson in strategic surprise. Atlantic Council. <https://www.atlanticcouncil.org/blogs/new-atlanticist/by-fusing-intelligence-and-special-operations-israels-strikes-on-iran-are-a-lesson-in-strategic-surprise/>.

These two attacks could provide a rough inspirational blueprint for similar potential attacks on military installations and their defense communities in the United States. Granted, the attacks conducted by both Ukraine and Israel were incredibly well-planned, well-resourced, and executed by the highest level of military and intelligence professionals. They required months, if not years, of preparation. However, the attacks were also strategic in scope, striking multiple geographically separate targets simultaneously. Non-state actors, homegrown terrorists, or agents of competitor states could utilize the same general model of attack against a single, less complex target on United States soil (for example, a single installation's flight line, communications node, fuel storage tanks, or headquarters facility) or merely utilize drones to surveil military installations, setting conditions for a larger, more conventional attack. This smaller scope of incursion or attack could still yield potentially devastating and expensive results for U.S. military readiness at a comparatively low cost with a far lower logistical burden. Given the successful examples demonstrated to high acclaim, it would be naïve to think that America's enemies are not planning similar attacks against military installations within the United States.

This threat is even more critical because drone incursions around U.S. military installations are already a demonstrated issue. The previous article in this series describes General Gregory Guillot, Commander of U.S. Northern Command (NORTHCOM), who testified<sup>5</sup> before the Senate Armed Services Committee in April 2025 that over 350 unauthorized drone detections across 100 different military installations occurred in 2024. The situation has only become more critical. In the fall of 2025, NORTHCOM representatives stated<sup>6</sup> that drone sightings had jumped by 82 percent from 2024 to 2025. Gen. Guillot himself noted, "I don't know if the problem's worse, or we have more systems out there that can detect them." Of course, significant progress is being made in detection, deterrence, and response to drone incursions, but it should be clear to all stakeholders that additional work is needed if U.S. military installations expect to successfully defend

against a drone-based attack from a determined enemy. However, the biggest impediment to further progress in drone response does not concern the technology or military capability for response, but rather the policies that enable response.

## THE CRITICAL QUESTION: HOW TO ENABLE EFFECTIVE RESPONSE?

### Key Takeaways

- The U.S. military's ability to respond to drone incursions and threats is mired in conflicting directions and overlapping authorities from multiple federal sources.
- Defense communities and their local installation partners are almost certain to encounter procedural barriers and regulatory challenges as they seek to develop solutions to drone-related threats.

It's well-known that the U.S. military operates with significant restraint in domestic environments due to the principles of the Posse Comitatus Act. The Act itself is a bedrock institution that we certainly cannot fault; however, it does present legal challenges for an installation's response to drone incursions. Drones can move from an airspace governed by civilian authorities to one governed by military authorities in seconds, even if its operator does not have hostile intent. And even if a suspicious drone is over military airspace, its operator may not be within a military installation boundary. If this is the situation, any attempts to investigate or apprehend an operator lie firmly within the jurisdiction of local law enforcement.

Ideally, installation leadership should have clear authority to respond to a drone incursion once it firmly identifies the drone as a threat, but the reality is much more complex. Multiple federal agencies including the Department of Homeland Security (DHS), FAA,

5 Securing The Skies: Addressing Unauthorized Drone Activity Over U.S. Military Installations Hearing Before the Subcommittee On Military And Foreign Affairs of the Committee On Oversight And Government Reform U.S. House Of Representatives One Hundred Nineteenth Congress First Session. (2025). <https://www.congress.gov/119/meeting/house/118165/documents/HHRG-119-GO06-Transcript-20250429.pdf>.

6 Marrow, M. (2025, October 10). With daily drone incursions over bases, NORTHCOM takes aim through Falcon Peak. Breaking Defense. <https://breakingdefense.com/2025/10/drone-incursions-us-military-falcon-peak-2025-cuas/>.

and state and local law enforcement entities have jurisdictional claims over airspace, as well as drone detection and response procedures. Many agencies and entities are also stakeholders in the development of counter-drone technologies and procedures. This system of overlapping authorities translates into a confusing morass of responsibilities and connections for installations and their civilian counterparts on the other side of their fence lines.



- **FAA:** The lead rulemaking agency for small drone operations, registration, and certification per 14 U.S.C. § 107<sup>7</sup> and the Executive Order (EO) titled “Unleashing American Drone Dominance”<sup>8</sup> (June 2025). The FAA also leads homeland security and national security assessments per the EO titled “Restoring American Airspace Sovereignty” (June 2025)<sup>9</sup>.
- **Department of Energy (DOE):** The 2017 National Defense Authorization Act gave the National Nuclear Security Administration (NNSA) within the DOE the authority to protect its facilities from unauthorized drones that pose potential threats to the safety or security of assets or personnel.<sup>10</sup>
- **10 U.S.C. § 130i:** This statute, enacted in 2016, allows for the designation of high-risk Department of War (DOW) facilities and for the DOW to detect, track, and mitigate drone threats to those facilities.<sup>11</sup>
- **DHS:** As of January 2026, the Program Executive Office for Unmanned Aircraft Systems and Counter-Unmanned Aircraft Systems will oversee strategic investments in drone and counter-drone technologies.<sup>12</sup>

7 Federal Aviation Administration. (2016, June 28). 14 CFR Part 107 – Small Unmanned Aircraft Systems. [www.ecfr.gov](https://www.ecfr.gov). <https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-107>.

8 Unleashing American Drone Dominance. (2025, June 6). The White House. <https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/>.

9 Restoring American Airspace Sovereignty. (2025, June 6). The White House. <https://www.whitehouse.gov/presidential-actions/2025/06/restoring-american-airspace-sovereignty/>.

10 National Nuclear Security Administration. (2021, September). Counter Unmanned Aircraft Systems. <https://www.energy.gov/sites/default/files/2021-09/20210928%20-%20Counter%20UAS.pdf>.

11 10 U.S. Code § 130i - Protection of certain facilities and assets from unmanned aircraft. (n.d.). LII / Legal Information Institute. <https://www.law.cornell.edu/uscode/text/10/130i>.

12 Department of Homeland Security Launches New Office to Advance Drone and Counter-Drone Technologies | Homeland Security. (2025). U.S. Department of Homeland Security. <https://www.dhs.gov/news/2026/01/12/department-homeland-security-launches-new-office-advance-drone-and-counter-drone>.

- **DOW:** The Joint Interagency Task Force 401 (JIATF-401) was established in August 2025<sup>13</sup> as a replacement for the Joint Counter-small Unmanned Aircraft Systems Office. It has been designated as a direct reporting entity to the Deputy Secretary of War and will lead and synchronize DOW efforts to counter small unmanned systems. JIATF-401 released updated guidance<sup>14</sup> on January 26, 2026, that stated an intent to further empower installation commanders with the authority to protect military assets, including streamlining the processes of 10 U.S. Code § 130i.
- **NORTHCOM:** NORTHCOM is the designated synchronizer for DOW’s Homeland Counter-small Unmanned Aircraft Systems (HC-sUAS)<sup>15</sup> operations in CONUS and Alaska.
- **Department of Justice (DOJ):** The Counter-UAS Authority Extension Act authorized the DHS and DOJ to detect, identify, monitor, and track drones and use reasonable force against drones deemed to pose a threat to certain facilities and assets, but this authority lapsed at the end of Fiscal Year (FY) 2025.<sup>16</sup>
- **State and Local Governments:** These entities may not regulate aviation safety or airspace efficiency but are allowed by the FAA to “generally regulate outside those fields”.<sup>17</sup> Additionally, the Safer Skies Act<sup>18</sup> within the 2026 National Defense Authorization Act (NDAA) provides additional frameworks for state and local governments to “take actions necessary to mitigate a credible threat” posed by drones to people or facilities. If this act is adopted, local and state law enforcement and other entities such as correctional facilities

will have the ability to conduct drone mitigation activities using federally approved methods and training after completion of federally mandated requirements

- **Additional Federal Laws:** Federal legislation also impacts the landscape of authorities surrounding drone operations. The Drone Espionage Act, recently advanced to the full Senate by the Senate Judiciary Committee, aims to prevent drones from taking unauthorized videos of U.S. military installations and close loopholes for law enforcement to take action against drones suspected of recording installations. If passed, this bill will add to the various permissions and authorities that exist to empower action against suspected hostile drone operations.<sup>19</sup>



13 U.S. Department of Defense. (2025, August 27). Establishment of Joint Interagency Task Force 401. <https://media.defense.gov/2025/Aug/28/200379002/1/-1/0/ESTABLISHMENT-OF-JOINT-INTERAGENCY-TASK-FORCE-401.PDF>.

14 JIATF-401 Announces Updated Guidance to Counter Drone Threats in the Homeland. (2026). U.S. Department of War. <https://www.war.gov/News/Releases/Release/Article/4389392/jiatf-401-announces-updated-guidance-to-counter-drone-threats-in-the-homeland/>.

15 Homeland C-sUAS. (2024). Northcom.mil. <https://www.northcom.mil/Missions/Homeland-Defense/Homeland-C-sUAS/>.

16 D-MI, G. C. (2023). S.5639 - 118th Congress (2023-2024): Counter-UAS Authority Extension Act. Congress.gov. <https://www.congress.gov/bill/118th-congress/senate-bill/5639>.

17 U.S. Department of Transportation. (2023, July 14). Updated Fact Sheet (2023) on State and Local Regulation of Unmanned Aircraft Systems (UAS). Office of the Secretary of Transportation General Counsel. <https://www.faa.gov/sites/faa.gov/files/State-Local-Regulation-of-Unmanned-Aircraft-Systems-Fact-Sheet.pdf>.

18 D-MI, G. C. (2025). Text - S.3481 - 119th Congress (2025-2026): SAFER SKIES Act. Congress.gov. <https://www.congress.gov/bill/119th-congress/senate-bill/3481/text/is>.

19 Staff Reports. (2026, February 23). Drone Espionage Act Hits Home on the Emerald Coast - Mid Bay News. Mid Bay News. <https://midbaynews.com/post/drone-espionage-act-hits-home-on-the-emerald-coast>.

These overlapping authorities are complex enough to puzzle even the agencies that are assigned to execute specific tasks in drone detection and response. In January 2026, the Department of War’s Inspector General released an advisory report on the protection of critical DOW assets (those covered under 10 U.S.C. § 130i) against drone incursions. This report found that the DOW did not provide clear policy for designating which facilities fell under 10 U.S.C. § 130i and that internal policies to approve the use of drone countermeasures were not standardized between the services. The report states:

***“DoD officials issued over 20 policies regarding C-UAS that: did not provide clear policy for the use of C-UAS capabilities for all military installations within the United States and its territories; did not sufficiently standardize policy for the section 130i package; and allowed the Services to develop different policies and procedures for prioritizing the deployment of C-UAS capabilities.”<sup>20</sup>***

In short, defense communities seeking to partner with their installation counterparts on drone mitigation can expect, in the immediate term, to encounter a complex regulatory environment that could present obstacles to solving drone-related challenges.



## When Authorities Collide

In early February 2026, airspace over El Paso, Texas was abruptly closed by the FAA.<sup>21</sup> Although the initial announcement declared a 10-day shutdown, this was reversed hours later and El Paso’s airport quickly resumed regular operations. However, even this small closure affecting only 14 commercial flights cost the City of El Paso an estimated \$1.5 million in lost economic impact.<sup>22</sup> This cost is especially irksome as the cause of the shutdown can be traced directly to poor coordination in anti-drone measures. Although some exact details are still unknown, the understood sequence of events is that Customs and Border Protection officers utilized an anti-drone laser near El Paso’s Fort Bliss without properly informing the FAA of their intent to conduct operations. In response to the unknown activity, the FAA closed the airspace to ensure commercial air safety.<sup>23</sup> There is also little understanding of why the anti-drone laser was utilized, though the Department of Transportation Secretary indicated it was deployed to “address a cartel drone incursion”.<sup>24</sup> While the aftermath of this case and any subsequent investigations should provide more information, the overall sequence of events is a prime example of how different entities acting with various authorities have the potential to negatively impact defense communities if not properly coordinated or if operations are misaligned.

- 20 U.S. Department of Defense. (2026, January 20). Immediate Attention Required to Protect DoD Covered Assets Against Unmanned Aircraft Systems (UAS) Report No. DODIG-2026-045. Office of Inspector General, Department of Defense. [https://media.defense.gov/2026/Jan/21/2003858370/-1/-1/1/DODIG-2026-045\\_REDACTED%20SECURE.PDF](https://media.defense.gov/2026/Jan/21/2003858370/-1/-1/1/DODIG-2026-045_REDACTED%20SECURE.PDF). Page 5.
- 21 Kim, S. M., Finley, B., Jalonick, M. C., Lee, M., & Funk, J. (2026, February 11). Dispute over laser tests led to El Paso airspace closure, AP sources say. AP News. <https://apnews.com/article/faa-el-paso-texas-air-space-closed-1f774bdfd46f5986ff0e7003df709caa>.
- 22 Moore, R., Perez, E. S., & Perez, D. (2026, February 11). FAA lifts unprecedented El Paso airspace restrictions after seven hours; 14 flights canceled. El Paso Matters. <https://elpasomatters.org/2026/02/11/unexplained-faa-order-shuts-down-el-paso-southern-new-mexico-airspace-for-10-days/>.
- 23 Cox, M. (2026, February 14). Airspace Shutdown Is “Case Study” in Complex Counter-Drone Ops. Air & Space Forces Magazine. <https://www.airandspaceforces.com/el-paso-airspace-shutdown-complexity-counter-drone-ops/>.
- 24 Secretary Sean Duffy. (2026). X (Formerly Twitter). <https://x.com/secduffy/status/2021594420806639787?s=43>

# SOLUTIONS: WHAT DOES SUCCESS LOOK LIKE?

## Key Takeaways

- **Installation-community partnerships have multiple actions at their disposal that will assist military installations in mitigating drone threats. Most importantly, these partnerships should continue to act as connectors between military, state, local, and federal agencies to ensure a collaborative, holistic response to local drone threats.**
- **The Safer Skies Act within the 2026 NDAA enables state and local entities to take a larger role in drone detection and mitigation over critical infrastructure. Installation-community partnerships should assist local law enforcement and other local stakeholders to be prepared to assume these duties and interact with this Act's new processes once it becomes law.**

Despite the complexities of responding to the unique threats posed by drones, there are multiple actions that installation-community partnerships can take to help safeguard critical military-civilian shared infrastructure and support national security objectives. These actions help answer one or more of the critical questions that together summarize the major challenges of countering drone threats:

**How can military installations and their community partners enable swift identification of deliberate, hostile drone incursions?**

**Once identified, how do installations and their community partners rapidly engage and neutralize drone incursion threats with an appropriate response?**

And, perhaps most importantly,

**How can installations and their community partners proactively deter drone incursions?**

Installations and their partner defense communities have vastly different security requirements, which are affected by many factors such as local geography, nearby population centers, military mission types, and federal, state and local regulations. The differences in these requirements also provide different capabilities and possibilities for resource coordination against drone threats. Because of this situational variability, it is likely that there will never be a one-size-fits-all blueprint for installation-community action against drone threats. However, this mindset should be freeing, not restrictive. Installation-community partnerships should purposefully approach the complexity of drone threats through a local lens, cooperating on issues that can solve immediate, localized problems and building coordination between local law enforcement, government entities, and on-the-ground commanders of military and federal assets in the area. These locally driven actions can provide innovative, customized best practices that will collectively “move the needle” in drone threat education, identification, protection, and response.

## Host or participate in drone response exercises and drills:

Training exercises involving local community law enforcement or emergency services, their military counterparts, and other federal or state entities are useful to provide insight into the techniques and



capabilities that exist to deter and mitigate drone incursions. Particularly important is the ability of the exercises to identify threat zones and prioritized risk assessments for critical assets and infrastructure. Many states, installations, and federal agencies run exercises from tabletop drills to full-scale wargames designed to test different counter-drone tools and gather information on response situations. These exercises are incredibly valuable methods to generate further understanding of drone threats and their mitigation, but larger exercises conducted by the National Guard or federal agencies should not replace point-to-point coordination between defense communities and local installations. It is most important for local authorities to understand each other's Standard Operating Procedures and have clearly designated lines of communication, authorities, and resources for drone detection, deterrence, and response. This understanding is best achieved through local exercises and direct coordination.

**Case Study: The Civil Air Patrol and Dover Air Force Base (AFB) partner for counter-drone testing.**<sup>25</sup>

In 2019, Dover AFB's 436th Airlift Wing tested counter-drone capabilities in a formal exercise through a partnership with the local Civil Air Patrol (CAP) and in coordination with other agencies including the FAA. In this exercise, the CAP used commercial drones to infiltrate the base, allowing the 436th Security Forces Squadron to practice locating and intercepting the UAS. This exercise was unique in that it utilized the base itself as a testing location in contrast to other installations that have used off-base locations. The event demonstrated the range of possibilities available through creative partnerships and how civilian organizations can be used to simulate non-military threats in collaborative exercises.

**Case Study: Tabletop Exercises as strategic tools.**

Tabletop Exercises (TTX) deserve a specific note as they provide a distinct process to simulate various hypothetical events and 'stress-test' existing systems and processes that rely on installation-community cooperation. These exercises require some resourcing and advanced planning but are significantly easier to organize than live-scale exercises and can be

customized for a variety of situations. In TTX, trained facilitators design "injects" to simulate operational disruptions, cascading failures, and other negative events which test integrated interdependencies between military and civilian infrastructure, authorities, and procedures. Because results are monitored and captured by facilitators, there are great opportunities to identify weakness and build stronger systems and processes after the TTX concludes. Several consultant firms including Matrix Design Group, Inc. are regular facilitators of TTX processes and have integrated them into Installation Readiness review projects for multiple installations such as Pine Bluff Arsenal, Arkansas and Joint Base San Antonio, Texas. These TTX have regularly produced results that help deconflict jurisdictions, define permissions and catalyze efforts to build common understanding of complex issues, exactly the results that will assist in countering drone threats.

## Formalize local-level authorities to drone response.

As mentioned in this article's earlier analysis, the FAA preempts local regulations on airspace safety and efficiency, but there can still be significant grey areas and situational contexts that fall under the jurisdiction of local authorities. All local entities should understand to the greatest extent possible the authority that is granted to local government officials, installation personnel, and other relevant stakeholders. This can be accomplished through a formal resolution or Memorandum of Understanding. Doing so will codify a baseline understanding of roles and responsibilities for drone incursion response and ensure that further cooperation can build off a level playing field.

**Case Study: Communities organize to support Wright-Patterson Air Force Base.**<sup>26</sup>

Last year, the Wright-Patterson Air Force Base Regional Council of Governments agreed to support its local installation by coordinating enforcement actions on a new state law designed to penalize unauthorized drone flights near military bases. This unification of local governments and police departments simplifies Wright-Patterson's lines of communication and helps stakeholders utilize

25 Welcome To Zscaler Directory Authentication. (2026). Af.mil. <https://www.amc.af.mil/News/Article-Display/Article/2024056/dover-afb-partners-with-delaware-cap-for-counter-uas-testing/>.

26 Gnaou, T. (2025, May 8). Cities surrounding Wright Patt responsible for enforcing new drone law. Dayton-Daily-News; Dayton Daily News. <https://www.daytondailynews.com/local/communities-responsible-for-drone-enforcement-wright-patt-council-told/V4NWPQRCHFEA3BLY5XH2MWEGXU/>.

shared capabilities. The action may have a limited scope and is less flashy than a regional exercise between law enforcement and uniformed personnel, but it helps answer critical questions on techniques and authorities and provides a measure of clarity to the current jurisdictional confusion in drone incursion response. These local-level nuts-and-bolts agreements are exactly where defense community organizations can best support their partner installations.

## Bridge communication and action between installations, local authorities, and other non-DOW federal assets.

Installation-community partnerships have long acted as the connective tissue between private and public stakeholders and military installations, in addition to serving as clearinghouses of information. Their ability to link entities and individuals from outside and inside installation fence lines and promote cooperation on local issues is a force multiplier against shared challenges. These partnerships should continue in this role and engage other non-DOW assets to support and enhance responses to drone threats or incursions. Since many federal agencies other than the DOW have parts to play in drone mitigation, coordinating with other federal assets such as FBI field offices and DHS Fusion Centers can unlock capabilities to assist with drone responses that would otherwise not be available to installations or their community counterparts. As with the previously stated example, this relationship-building doesn't necessarily make an engaging headline, but it does allow for more coordinated, more comprehensive, and, ultimately, more effective response to critical threats.

**Case Study: Aurora connects local police, federal agents, and local military responses to drone incursions.**<sup>27</sup> Last May, the Aurora City Council of Aurora, Colorado approved an agreement that enables cooperative investigation and enforcement of hostile drone incursions between the Aurora

Police Department, the local FBI, and Buckley Space Force Base's 460th Security Forces Squadron. The agreement outlines areas of responsibility in responding to civilian suspects and civilian-originated drone incursions on Buckley Space Force Base while encouraging mutual training exercises and public outreach on drone regulations.

## Advocate for legislative policy that will reduce complexity in drone response, clarify the implementation of the Safer Skies Act, and make more installations "covered" under the provisions of 10 U.S.C. § 130i.

Policymakers have widely acknowledged the overbearing complexity of laws and policies related to military-civilian responses to drone incursions and threats. The 2025 NDAA contained multiple provisions designating funds and authorities to coordinate drone responses and counter-UAS resources, and the Safer Skies Act within the 2026 NDAA further overhauls federal directives on drone response.<sup>28</sup> Installation-community partnerships can contribute to drone policy debates by continuing to do what they have successfully done for decades: advocating for select policy changes or resourcing on behalf of their joint military-civilian priorities. Specific targets for this advocacy could include the following:

- *Shaping the implementation of the Safer Skies Act and recent guidance from JIATF-401.* The Safer Skies Act directs federal agencies including the DOJ and DHS to issue implementation guidelines for the training that state and local entities must undergo before they can be certified to engage drone threats, as well as guidelines for the approved technology that can be utilized against drone threats. Additionally, guidance released from JIATF-401 on January 26, 2026, directs installation commanders to issue "installation-specific operating procedures"<sup>29</sup> on drone response and

27 Ballard, C. (2025, May 22). Aurora OKs agreement to tackle drone threats near Buckley Space Force Base. Sentinel Colorado. <https://sentinelcolorado.com/metro/aurora-oks-agreement-to-tackle-drone-threats-near-buckley-space-force-base/>.

28 Department of Defense Counter Unmanned Aircraft Systems: Background and Issues for Congress. (2025). Congress.gov. <https://www.congress.gov/crs-product/R48477>.

29 JIATF-401 Announces Updated Guidance to Counter Drone Threats in the Homeland. (2026). U.S. Department of War. <https://www.war.gov/News/Releases/Release/Article/4389392/jiatf-401-announces-updated-guidance-to-counter-drone-threats-in-the-homeland/>.

defense. Defense communities should utilize their advocacy networks to help shape the guidelines from both the Safer Skies Act and JIATF-401's initiatives and push for the inclusion of technology or tools that have been found to be successful during local exercises or drills.

- *Increasing the authority of installations with 10 U.S.C. § 130i.* The same 2026 DOW report that identified unclear and nonstandard processes between military services for designating “covered” facilities also identified instances where installations or facilities that were appropriate to be “covered” were not so designated. Coverage under 10 U.S.C. § 130i is currently the most straightforward method for a military installation to provide proactive defense against drone threats. Ideally, all assets that contain critical missions or perform critical functions that meet the conditions of the statute should be designated as covered. Installation–community partnerships can seek clarification on their local installation or federal facility’s coverage and make the case through legislative channels for why they require coverage. The DOW’s JIATF-401, in its late January release of new guidance, also indicated that it is pursuing streamlined processes for 10 U.S.C. § 130i designation or that it might provide completely new systems of authorities and decisive action permissions for installations. JIATF-401’s initiatives could create further openings for installation–community partnerships to pursue expanded 10 U.S.C. § 130i coverage.

For reference, nine mission areas are eligible for coverage, and an installation or facility hosting missions or infrastructure related to those missions can apply for coverage through their service. Those mission areas include:

- Nuclear deterrence;
- Missile defense;
- National security space;
- Protection of the Presidential line of succession;
- Air defense of the United States;

- Combat support agencies;
- Special combat operations activities;
- Production, storage, transportation, or decommission of high-yield explosive munitions; and
- Major range or test facility base.

## Identify and prioritize collaborative projects that increase drone incursion response capabilities on both sides of the installation fence line.

The Safer Skies Act (when passed) will create more opportunities to invest in local projects and joint capabilities for entities on both sides of an installation fence line. Installation–community partnerships should invest time now to proactively identify areas where funding or other resourcing could provide counter-UAS tools or other protection for shared infrastructure. Identified opportunities can then be translated into funding proposals as required when the Safer Skies Act provisions on training and approved technology and tools are clarified by federal agencies.

## A NOTE ON RESOURCING

As with most military–civilian partnership initiatives, resourcing and funding constraints limit the ability of local stakeholders to coordinate solutions to drone threats. However, the Safer Skies Act and other recent federal initiatives provide some promising possibilities for installation–community partnerships to seek funding for local counter-UAS or drone mitigation efforts. The following list provides initial recommendations for defense communities seeking funding for programs or projects to defend against drone threats:

**Department of Homeland Security’s Counter-Unmanned Aircraft Systems Grant Program:**<sup>30</sup> This new grant program, established under the One Big Beautiful Bill Act of 2025, provides funding for state, local, tribal, and territorial entities to detect, identify, track, and monitor drones and combat the unlawful use of drones that pose a threat to the safety and security of the American people, their communities, and their

30 Counter-Unmanned Aircraft Systems Grant Program Fact Sheet. (2025, November 12). Fema.gov. <https://www.fema.gov/fact-sheet/counter-unmanned-aircraft-systems-grant-program-fact-sheet>.

institutions. Its first year of existence, Fiscal Year 2026, saw \$250 million awarded to jurisdictions hosting National Special Security Events (NSSE), particularly those in support of the 2026 FIFA World Cup and preparations for America 250 celebrations. As a new program, the intricacies and recurring award criteria can be expected to shift from year to year, but this is a highly promising program that in the future could serve as a leading source of funding for community-based, military shared, drone mitigation projects.

#### **Department of Homeland Security's Grant**

**Programs:**<sup>31</sup> The DHS administers three individual award grant programs: the State Homeland Security Program, Urban Area Security Initiative, and Operation Stonegarden. While each grant program differs in topical areas (Operation Stonegarden, for example, is designed to provide funding to land or maritime border security efforts), all could be utilized to fund drone-related efforts that enhance preparedness and capabilities for the protection of specific targets such as military installations.

#### **DOW Office of Local Defense Community Cooperation**

**Installation Readiness Program:**<sup>32</sup> OLDCC's Installation Readiness Program is designed to assist states and communities in partnering with their local military installations to plan and enhance infrastructure and measures that contribute to maintaining or improving a military installation's readiness and lethality. Although not a drone-focused program, this is an ideal mechanism that communities and installations could use to engage in planning and project analysis on collaborative topics related to drone threats.

**State-Level Initiatives:** Multiple states including Texas<sup>33</sup>, California<sup>34</sup>, and Arkansas<sup>35</sup> provide grants for law enforcement or other entities that could be purposed to fund drone-related training, projects, or other collaboration efforts between defense communities and military installations. These grant opportunities are highly variable by state and by use case, but it is important to acknowledge their existence as non-federal programs available to defense communities and potentially suitable for drone-related initiatives.

## CONCLUSION

As shown by recent events, the emergent threat posed by drones and their unauthorized incursions into sensitive airspace and over military installations is no longer up for debate. The Safer Skies Act and other federal policy actions have furthermore shown that experts expect this threat to only grow with time. However, as discussed throughout this article, an installation's ability to respond to drone threats remains tangled in a confusing overlap of various federal agency authorities and permissions. To enable military installations to more effectively protect their missions and to allow them to coordinate with local partners on safeguarding shared infrastructure, more work is needed to cut through the noise and deliver actionable methods for hostile drone detection, identification, and response.

Installation-community partnerships are optimally positioned to lead this work and help military installations deliver safety to both their jointly utilized infrastructure outside the fence line and their missions inside the fence line. As drone threats utilize advanced technology to circumvent hardened perimeters and have no widely accepted counter, the best defense against them must be flexible, scalable, and, most importantly, localized to specific situations and geographic areas. Through their core strengths of stakeholder coordination, strong advocacy, and building trusted relationships, installation-community partnerships are perfectly positioned to develop these unique defenses and ensure that drone threats rapidly become a minor concern in military-civilian risk assessment throughout the United States.

31 FEMA. (2024, December 13). Homeland Security Grant Program | FEMA.gov. [www.fema.gov. https://www.fema.gov/grants/preparedness/homeland-security.](https://www.fema.gov/grants/preparedness/homeland-security)

32 Installation Readiness | Office of Local Defense Community Cooperation. (2024). Oldcc.gov. <https://oldcc.gov/our-programs/installation-readiness>

33 Grants. (n.d.). Gov.texas.gov. [https://gov.texas.gov/organization/financial-services/grants.](https://gov.texas.gov/organization/financial-services/grants)

34 Grants Central System | California Governor's Office of Emergency Services. (2024). Ca.gov. [https://www.caloes.ca.gov/office-of-the-director/policy-administration/finance-administration/grants-management/grants-central-system/.](https://www.caloes.ca.gov/office-of-the-director/policy-administration/finance-administration/grants-management/grants-central-system/)

35 Arkansas Department of Public Safety. (2020). Arkansas Department of Public Safety. [https://dps.arkansas.gov/?s=grants.](https://dps.arkansas.gov/?s=grants)



The Association of Defense Communities (ADC) builds resilient communities that support America’s military. It is the connection point for leaders from communities, states, the military and industry on community-military issues by enhancing knowledge, information sharing, and best practices. With nearly 300 communities, states, regions and affiliated industry organizations, ADC represents every major defense community/state in the nation.

[defensecommunities.org](https://defensecommunities.org)



Matrix Design Group is an award-winning interdisciplinary firm, providing professional engineering, consulting, environmental and planning and program management for both the public and private sectors. As specialists in sustaining installations, community advocacy and BRAC services, Matrix is a complete provider of innovation and solutions. With the industry’s most comprehensive experience, the Matrix team has the necessary expertise to assess installation closure susceptibility and the tools and knowledge to help defense communities remain vibrant.

[matrixdesigngroup.com](https://matrixdesigngroup.com)



Developed in collaboration with:



1300 Connecticut Ave NW  
Suite 200  
Washington, DC 20036  
[defensecommunities.org](http://defensecommunities.org)