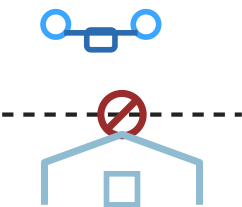


Principal Brief // two-minute read

- DRONES & AERIAL
- RESIDENTIAL EXPOSURE
- PHYSICAL SECURITY

You Are Not Allowed to Stop It



If a drone hovers over your house, nobody on your payroll may lawfully bring it down. Not your detail, not your security vendor, not you. That is a federal matter, and it is the single most important fact about this threat.

WHAT HAPPENED

Cheap attack drones are now made at industrial scale: Ukraine's security council says its industry can build more than eight million a year across 160 companies. And the model has been proven against civilians. In May 2025 a UN commission found that Russian forces committed crimes against humanity by using drones to hunt people in Kherson, killing nearly 150, with operators watching live video and dropping explosives on people walking to work or walking their dogs.

WHY IT REACHES YOU

Because the defense does not come with the threat. Jamming is what stops these drones in war, and operating a jammer is illegal here. Shooting one down, netting it, or hijacking its link runs into aircraft, wiretap and computer-crime law. When Congress widened counter-drone authority in December 2025, it gave it to trained police, not to the private market.

THREE THINGS TO TAKE FROM THIS

- 1

It is permission, not product

The systems work and exist. What a private party cannot obtain is the legal authority to use one.
- 2

Detection is lawful and useful

Watching, recording, and building a pattern is legal, and it is what makes an agency able to act.
- 3

Know who can press the button

It may now be your county police, if they have certified. Find out before you need them, not during.

DO THIS

- ☐ **YOU, WITH YOUR DETAIL**
Give a standing order that nobody interferes with a drone. The protective instinct here produces a federal charge.
- ☐ **YOU, WITH YOUR FAMILY OFFICE**
Buy detection, not mitigation, and ask what evidence it produces that an agency will actually use.
- ☐ **YOU, THIS MONTH**
Ask whether your local police have completed counter-drone certification, and record who to call.

NOT THE STORY YOU MAY HAVE HEARD

No weaponized drone has attacked a private home in the United States, and this brief does not predict one on a timetable. The capability and the precedent abroad are established; the domestic attack is an inference. The part that needs no forecasting is the law, which already governs what you may do about the drone overhead today.

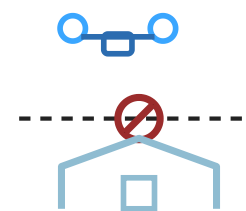
HOW SURE WE ARE

High on the capability, the documented use against civilians, and the legal position, which is statute rather than assessment. Moderate on any domestic timeline, and on how fast local agencies certify.

CB-059

The Airspace You Cannot Defend

"The drone is the cheap part. The authority to stop one is the part that is not for sale."



A small drone over a principal's house is a problem with an unusual shape. The capability to build and fly one is now industrial, cheap, and proven against civilians abroad. The capability to stop one exists and works. What a private principal cannot have, at any price, is permission to use it. Counter-drone mitigation in the United States is a federal authority granted to a short list of agencies, and the statutes that bar everyone else are aviation and wiretap law, not an oversight waiting to be corrected. A security program that plans to buy its way out of this is planning to buy an offense.

BLUF. Two things are true at once and the brief turns on holding both. First, the capability is real and at scale: Ukraine's National Security and Defense Council stated on 23 January 2026 that the country's industry can produce more than eight million FPV drones a year across more than 160 manufacturers, and the United Nations Independent International Commission of Inquiry on Ukraine concluded on 28 May 2025 that Russian forces had committed murder of civilians as crimes against humanity using drones in Kherson province, with nearly 150 civilians killed and hundreds injured since July 2024, operators watching live video feeds, selecting visibly civilian targets, and dropping explosives on them. The residential-target model is not hypothetical. Second, the defense does not transfer, and not because the market failed. Battlefield survival against these drones rests on electronic jamming, and operating a jammer in the United States is prohibited by the Federal Communications Commission, while disabling, seizing, or shooting down an aircraft, which a drone legally is, runs into 18 U.S.C. 32 on aircraft destruction, the Wiretap Act, and the Computer Fraud and Abuse Act.

The governing frame: mitigation is an authority, not a product. It sits with the Departments of Justice and Homeland Security under 6 U.S.C. 124n, the Department of Defense under 10 U.S.C. 130i, and the Department of Energy under 50 U.S.C. 2661. In December 2025 the SAFER SKIES Act, enacted in the FY2026 National Defense Authorization Act, extended detection and tracking plus limited disable-or-seize authority to trained state, local, tribal and territorial law enforcement, with the implementing rule effective 1 July 2026 and published on 6 July. Congress widened the circle to local police, and pointedly not to the private market. What a principal can lawfully own is detection, documentation, and a working relationship with whichever agency now holds the authority where they live. That is a smaller answer than a counter-drone system, and it is the one that does not end in a federal charge.

You can buy the sensor. You cannot buy the permission.

PRODUCTION AT SCALE · 23 JAN 2026

Ukraine's National Security and Defense Council stated that the country's defense industry has the capacity to produce more than eight million FPV drones a year, made by more than 160 companies, and called it an unprecedented figure for any country at war. Read it as capacity rather than as units delivered, which is how the council framed it. Russian output is comparable in order of magnitude. Whatever the exact production number in any given year, the manufacturing base, the component supply chain, the operator training pipeline, and the published build instructions all now exist at a scale that does not reverse when a war ends.

PROVEN AGAINST CIVILIANS · 28 MAY 2025

The United Nations Independent International Commission of Inquiry on Ukraine concluded that Russian armed forces committed murder of civilians as crimes against humanity using drones. From July 2024 onward, across Kherson city and sixteen localities, nearly 150 civilians were killed and hundreds injured. The commission described operators using real-time video from cameras on the drones, focusing on targets that were visibly civilian, and dropping explosives on them. A health professional quoted in the findings described attackers "chasing and hunting civilians who are on their way to work or walking their dogs." This is the part of the threat model that no longer requires inference: individual human beings, going about domestic routines, deliberately hunted by cheap drones.

WHO MAY ACT · STANDING FEDERAL LAW

Counter-drone mitigation authority in the United States is narrow and statutory. The Departments of Justice and Homeland Security hold it under 6 U.S.C. 124n for covered facilities and assets, the Department of Defense under 10 U.S.C. 130i for its own installations, and the Department of Energy under 50 U.S.C. 2661 for certain nuclear facilities. Each is bounded by facility, by threat finding, and by coordination requirements with the Federal Aviation Administration. None of them covers a private residence as such.

THE CIRCLE WIDENED, BUT NOT TO YOU · DEC 2025 TO JUL 2026

The SAFER SKIES Act, enacted in December 2025 as part of the FY2026 National Defense Authorization Act, extended counter-drone authority to state, local, tribal and territorial law enforcement and correctional agencies that are properly trained, allowing them to detect, track, and in limited circumstances disable or seize a drone. The Justice and Homeland Security interim final rule took effect on 1 July 2026 and was published on 6 July, with a two-tier training regime: Tier 1 by online certification, Tier 2 in person at the FBI's National Counter-UAS Training Center. Counter-drone vendors must submit their products for federal review to appear on the authorized list. Private entities received no authority in any of it. The practical consequence is local: the agency that can lawfully act near a principal's home may now be the county sheriff rather than a federal team, if that agency has done the training.

A RENEWABLE AUTHORITY, NOT A PERMANENT ONE · OCT 2025

The federal counter-drone authority lapsed during the government shutdown that began in October 2025, because it is periodically reauthorized rather than standing. That is worth knowing for planning: the set of people lawfully able to bring down a drone over an American neighborhood is not fixed, and has been briefly empty in living memory.

SO WHAT The attack side of this is cheap, industrial, and already used to hunt civilians. The defense side is a federal permission that a family office cannot obtain, and the December 2025 expansion handed it to trained police rather than to the private market.

THE MECHANISM // WHY THE BATTLEFIELD ANSWER DOES NOT TRANSFER

THE DEFENSE THAT WORKS IS THE ONE THAT IS ILLEGAL HERE

What defeats these drones in Ukraine is electronic warfare: jamming the control link and the video downlink, and increasingly jamming satellite navigation. In the United States, operating, marketing, or importing a signal jammer is prohibited outright by the Federal Communications Commission, without a private exception to apply for. So the single most effective countermeasure in the war is the one countermeasure a principal categorically cannot deploy at home, and the gap is regulatory rather than technical.

The instinct to shoot one down, net it, or take over its control link runs into a body of law written for aviation and communications. Damaging or disabling an aircraft implicates 18 U.S.C. 32; intercepting the control or video link implicates the Wiretap Act; taking over the flight controller implicates the Computer Fraud and Abuse Act. These are felonies, and the fact that the aircraft was over the principal's own garden at the time does not resolve any of them. A security team acting on instinct in the moment converts a surveillance incident into a federal case with the principal's name on it.

THE PROCUREMENT TRAP THIS CREATES

A vendor offering residential drone defense is, in most configurations, offering a capability the client cannot lawfully operate. Detection is different and is lawful: passive radio-frequency sensing, acoustic detection, and optical tracking do not touch the aircraft. Under the new rule the mitigation systems themselves must pass federal review to be listed as authorized, and the list is for authorized agencies. The question to ask a vendor is not what the system can do but who, specifically and by statute, is permitted to press the button, and the honest answer for a private residence is nobody on the client's payroll.

WHAT DETECTION ACTUALLY BUYS

It is not a consolation prize. Detection provides the warning interval that lets people move away from windows and gardens, which is the entire protective action available during an overflight. It produces the evidence record, time, track, and radio signature, that turns a series of complaints into a case an authorized agency will act on. It distinguishes a hobbyist from a repeating pattern, which is the distinction that determines whether this is a nuisance or reconnaissance. And it identifies the approach corridors that matter for where a principal sits, walks, and parks.

THE TARGETING INPUT IS STILL THE CHEAP INTERDICTION POINT

A drone has to be flown to a place. Everything in CB-058 applies unchanged: the address, the property layout visible in listing photographs and aerial imagery, the routine, and the family's other locations are the inputs that make an overflight possible in the first place. This is the same argument as the ground case, and it is the only stage of the sequence where a private party retains full freedom of action.

FIGURE 1 // WHO MAY LAWFULLY DO WHAT, AS OF JULY 2026

ACTOR	DETECT AND TRACK	DISABLE OR SEIZE	AUTHORITY OR BAR
DOJ AND DHS	Yes, at covered facilities	Yes, on a credible-threat finding	6 U.S.C. 124n, with FAA coordination
DEPARTMENT OF DEFENSE	Yes, at its own assets	Yes, at its own assets	10 U.S.C. 130i
DEPARTMENT OF ENERGY	Yes, at certain nuclear sites	Yes, at those sites	50 U.S.C. 2661
TRAINED STATE AND LOCAL POLICE	Yes, once certified	Limited circumstances, once certified	SAFER SKIES Act, rule effective 1 Jul 2026; two-tier training
UNTRAINED LOCAL POLICE	Passive detection only	No	Same statutes that bind private parties
PRIVATE SECURITY AND THE PRINCIPAL	Yes, passive detection is lawful	No, at any price	18 U.S.C. 32, Wiretap Act, 18 U.S.C. 1030, FCC jammer prohibition

DETECT PASSIVELY	Radio-frequency, acoustic, or optical detection that observes without touching the aircraft. Lawful, and it is what creates every option below.
DOCUMENT	Time, duration, track, altitude, direction of approach and departure, and any radio identification the sensor captures. A pattern across weeks is what an agency can act on; a single annoyed phone call is not.
HARDEN OBSERVATION	Treat overhead sightlines the way you treat ground ones: where the principal is visible from above, which windows and outdoor areas are exposed, and what the property discloses in listing photography and aerial imagery.
ESTABLISH THE RELATIONSHIP	Find out now whether the local law-enforcement agency has completed SAFER SKIES certification and at which tier, because that determines who can act and how fast when it matters.
REPORT CORRECTLY	Know which agency takes the report in your jurisdiction and what evidence they need. This is a five-minute question to answer in advance and an impossible one to answer during an incident.

► THE PRACTICAL TEST

Ask any drone-defense vendor one question: *who on my staff is legally permitted to activate this, and under which statute?* If the answer is not a name and a citation, the system is evidence of intent to commit a federal offense.

THE STEELMAN // THE CASE THAT THIS IS OVERSTATED

THE BEST CASE FOR THE OTHER SIDE

- + There is no documented case of a weaponized commodity drone attacking a private residence in the United States. The residential threat remains an inference from a foreign war, and inference is not a fact.
 - + Weaponizing and delivering a drone against a specific person requires intent, skill, and a willingness to commit a capital crime, and the overwhelming majority of drone activity over homes is hobbyists, real-estate photography, and delivery.
 - + Fear of this threat is commercially useful to a category of vendor, which is a reason to discount the loudest voices describing it.
- All three hold, and the third is the reason this brief spends more space on what is lawful than on what is frightening. The response is that the two halves of the argument have different confidence levels and should be read separately. That commodity drones are produced at industrial scale and have been used to hunt civilians is established, and that mitigation is a federal authority private parties do not hold is a matter of statute, not forecasting. Only the residential-attack horizon is an inference, and the brief marks it as one. The practical consequence does not depend on the inference at all: a principal who is overflown today, by a hobbyist or by someone conducting reconnaissance, already needs to know who may lawfully act and what evidence that person needs. Most do not know, and finding out costs nothing.

FIGURE 3 // ANALYTIC CONFIDENCE BY CLAIM

Small attack drones are produced at industrial scale and the capability persists beyond the war.	STRONG / UKRAINE NSDC, 23 JAN 2026
Cheap drones have been used deliberately to hunt and kill civilians going about domestic routines.	STRONG / UN COMMISSION OF INQUIRY, 28 MAY 2025
Private parties hold no counter-drone mitigation authority and face felony exposure if they act.	STRONG / STATUTE
The December 2025 expansion went to trained law enforcement, not to the private market.	STRONG / SAFER SKIES ACT AND THE JULY 2026 RULE
Passive detection is lawful and is the principal's only owned control.	STRONG / STATUTE, BY EXCLUSION
A weaponized drone attack on a private residence in the United States within a near-term horizon.	MODERATE / INFERENCE FROM FOREIGN USE AND CAPABILITY, NO DOMESTIC CASE
How quickly local agencies will complete certification in any given jurisdiction.	MODERATE / VARIES BY AGENCY, AND MUST BE CHECKED LOCALLY
The gap is that no residential counter-drone product category exists.	REJECTED / THE SYSTEMS EXIST; THE PERMISSION TO OPERATE THEM IS WHAT A PRIVATE PARTY LACKS

POSTURE

FOR PRINCIPALS

- Treat overhead as an observed space rather than a defended one, and plan on that basis: where you are visible from above, and what a camera at two hundred feet sees of your routine, your vehicles, and your household.
- Do not let anyone on your staff or your detail improvise against a drone. Shooting, netting, or jamming one is a federal matter, and the instinct that feels protective in the moment produces the charge.

FOR FAMILY OFFICES

- Buy detection, not mitigation, and evaluate it as an evidence instrument: what it records, in what format, and whether an agency can use the output. A sensor whose output nobody will act on is a doorbell.
- Find out this month whether the local police agency has completed SAFER SKIES certification and at what tier, and record who to call and what they need. That single answer determines the real response time.
- Carry the CB-058 work forward to the air: the address, the aerial and listing imagery of the property, and the routine are what make an overflight worth attempting. That remains the stage where you retain full freedom of action.

- Write the drone incident protocol before you need it: who observes, who records, who calls which agency, what is preserved, and the explicit standing instruction that no one interferes with the aircraft. Brief the detail on the statutes by name, because a general prohibition is easier to ignore than a citation.
- Screen vendors against the authority question rather than the capability question, and treat any residential offer that includes jamming, spoofing, capture, or takeover as disqualifying rather than premium. Note also that the federal authority is periodically reauthorized and lapsed once during the October 2025 shutdown, so a continuity plan should not assume it is always in force. This is intelligence analysis, not legal advice, and the application of these statutes to a specific incident is a question for counsel.

CONFIDENCE High on the capability and precedent, which rest on the Ukrainian National Security and Defense Council's own statement of production capacity and on the findings of the UN Independent International Commission of Inquiry on Ukraine. High on the authority map, which is statute and published rulemaking rather than assessment. Moderate on any near-term horizon for a weaponized drone attack on a private residence in the United States, which remains an inference from foreign use and available capability with no documented domestic case, and no timetable is offered here, because nothing in the public record establishes one. Moderate on local agency readiness, which varies and must be checked jurisdiction by jurisdiction. The Ukrainian figure is capacity as stated by the council, not verified units delivered, and unit-cost figures circulating in trade coverage were not independently confirmed and are therefore not quoted here.

METHOD Revised edition. First published 3 May 2026; facts re-verified and analysis revised 11 September 2026. The previous edition located the problem in a missing product category and advised tracking the emerging residential counter-drone market. That is the wrong diagnosis and the advice would lead a family office to buy a system it cannot lawfully operate, so this edition rebuilds around the authority question: who may act, under which statute, and what remains lawful for a private party. It adds the statutory map, the SAFER SKIES expansion and its implementing rule, the October 2025 lapse, the lawful playbook, and the vendor test, and it removes the unsupported horizon figure and the unverified unit price. Cross-read against CB-058, CB-076, CB-077, and CB-078.

SOURCES [National Security and Defense Council of Ukraine on FPV production capacity](#) (23 January 2026). [UN Independent International Commission of Inquiry on Ukraine, findings on drone attacks against civilians in Kherson province](#) (28 May 2025). Counter-UAS authorities at 6 U.S.C. 124n, 10 U.S.C. 130i and 50 U.S.C. 2661; restrictions at 18 U.S.C. 32, the Wiretap Act and 18 U.S.C. 1030; FCC prohibition on signal jammers. [Crowell & Moring on the DOJ and DHS interim final rule implementing the SAFER SKIES Act](#) (effective 1 July 2026, published 6 July 2026). [DroneLife on the October 2025 lapse in federal counter-UAS authority](#). [Congressional Research Service on law enforcement and the counter-UAS landscape](#).

Scope note: this brief addresses small commodity drones over residential property in the United States. It does not assess military counter-UAS doctrine, and it does not advise on any specific incident, where the application of aviation and communications law is a question for counsel. Statutory authorities change: the federal counter-drone authority is periodically reauthorized and the state and local rule is an interim final rule subject to revision. Production figures are the issuing government's own statements of capacity. This is intelligence analysis, not legal advice.

OBSCUREIQ INTERNAL ANALYSIS // ARCHIVE COMM-059-DRONES-RESIDENTIAL-THREAT-2026Q2 // XREF **CB-058 CB-076 CB-077 CB-078** // ACCESS PUBLIC · PUBLIC-INTEREST RELEASE · REVISED 11 SEP 2026