
Sovereign Clean Sky

Mandatory cryptographic identity for every aircraft in U.S. airspace — and a default posture of "no valid token, no legitimacy."

Concept brief and infrastructure map Born Between 2 Generals •

cleansky.bornbetween2generals.com Prepared August 30, 2026

The idea in one paragraph

Every drone operating over the United States — commercial, hobbyist, law enforcement, and federal/military — carries a cryptographically verifiable identity token bound to a registered entity: a person, an organization, or an agency. The token is not a label; it is a signing key. A drone proves in flight, continuously, that it possesses the private key for a registered identity, and that the identity was endorsed by a legitimate registry. Anything airborne that cannot produce a valid, live, non-replayable proof is by definition unaccountable.

Unaccountable aircraft are **mapped first, then captured — not destroyed**. The leftover contacts, the ones that cannot prove themselves, are tracked continuously while interceptor drones launch, net them in mid-air, and tow them intact to a recovery point. The captured airframe becomes government property and forensic evidence: flight logs, SD card, payload, and control history, all intact, all attributable. The point is not surveillance and it is not firepower. The point is that a clean, attributable sky makes an unattributable aircraft instantly visible, physically removable, and *prosecutable* — and prosecution with a recovered airframe in evidence is what produces deterrence.

That is a real and coherent architecture. Below is what infrastructure it actually is, what already exists, and where the genuine gap sits.

Which infrastructure this is

This is not one system. It is five layers, and the U.S. already operates four of them in partial form.

LAYER	FUNCTION	CURRENT U.S. STATUS
1. Identity & registry	Issue cryptographic identities to aircraft, operators, and organizations; maintain revocation	Registration exists; cryptographic identity does not
2. Broadcast attestation	Aircraft continuously proves possession of its key over the air	Broadcast exists (Remote ID); authentication does not
3. Network aggregation	Collect, correlate, and distribute airspace picture to authorized parties	Partial — UTM / UAS Service Suppliers, Network Remote ID trials
4. Detection & correlation	Match what sensors see against what the sky claims; flag mismatches	Fragmented across DoD, DHS, DOJ, SLTT
5. Capture & attribution	Intercept, net, tow, and seize the airframe intact; preserve evidence for prosecution	Authority exists; hardware is combat-proven; not integrated to identity
6. Sovereign Fleet & forensics	Encrypted air-gapped interceptors that collect forensic evidence in flight; pattern-of-targeting analysis	Does not exist — this is the original contribution

Your instinct that this is simultaneously aviation infrastructure *and* national security infrastructure is correct, and it is exactly why it has been hard to build: layers 1–3 belong to the FAA and the Department of Transportation, layers 4–5 belong to DHS, DOJ, and DoD, and the handoff between them is where the concept lives or dies.

What already exists

The "digital license plate" is already federal law

Since 2021, codified at [14 CFR Part 89](#), most drones operating in U.S. airspace must broadcast identification and location in flight. Per the [FAA's Remote ID guidance](#), this covers every drone that is FAA-registered or requires registration — all Part 107 operations, and recreational drones over 0.55 lbs under Section 44809. Compliance became mandatory September 16, 2023 ([FAA talking points](#)).

Under the [Remote ID final rule](#), an operator broadcasts either the aircraft serial number or a **Session ID** — a rotating alternative identifier intended to give the operator privacy while still allowing authorities to resolve the identity through the registry. That Session ID mechanism is, structurally, very close to the "everyone gets a token, and it's for their benefit" idea you described: public observers see a pseudonym, authorities can resolve it.

So the tokenization mandate is not a new legal concept. **It already exists. It is just cryptographically hollow.**

The critical flaw — and it is exactly the one you're pointing at

Remote ID broadcasts are transmitted **in clear text with no authentication**. This is not a fringe criticism; it is the consensus finding of the security literature:

- Current standards "leave authentication mechanisms unspecified, enabling spoofing, relay, and replay attacks," and Remote ID "remains critically incomplete from a security perspective" ([arXiv, Tesla-authenticated Broadcast Remote ID](#)).
- Remote ID "lacks basic security mechanisms. Similar to ADS-B used in air traffic management, no authentication or encryption is mandatory," making it susceptible to spoofing and replay attacks that researchers have demonstrated with a Raspberry Pi ([Linköping University vulnerability study](#)).
- Remote ID "transmits plain-text messages, which creates an inherent vulnerability," fundamentally the same weakness as ADS-B ([peer-reviewed survey of ADS-B and Remote ID security](#)).
- Working spoofers are public. An [open-source Remote ID spoofer](#) broadcasts fake drone identities over Wi-Fi, single or multiple aircraft, at arbitrary locations.

This is the whole problem. A sky where every drone broadcasts an unsigned ID is not an accountable sky. A hostile operator broadcasts a stolen or invented ID and becomes indistinguishable from a delivery drone. Worse, an adversary can flood the picture with thousands of fake aircraft and destroy the operator's ability to trust any of it. Under today's rule, "it's broadcasting an ID" proves nothing — so the "if it has no token, take it down" trigger cannot be safely armed, because the token is forgeable in both directions.

The cryptographic layer you're describing is already a published standard

This is the most important finding in this brief. The IETF has a chartered working group — **DRIP, Drone Remote ID Protocol** — whose stated goal is "to specify how RID can be made trustworthy" ([IETF DRIP charter](#)). It has shipped:

- **RFC 9153** — DRIP requirements and terminology (February 2022).
- **RFC 9374** — the **DRIP Entity Tag (DET)**: a cryptographic identifier derived from a hierarchical Host Identity, so the identifier *is* a public-key commitment rather than an arbitrary string.
- **RFC 9575** — Standards Track, June 2024. Defines Broadcast RID Authentication Messages that cryptographically verify a message "was signed by the registered owner of the claimed DRIP Entity Tag," that the aircraft **possesses the private key** by signing data that is unique and unpredictable (defeating replay), and that a **chain of registered entities endorses** the identity through Broadcast Endorsements.
- **RFC 9886** — DRIP registries.

- **IANA DRIP registry** — assigned code points, including signature suites (ECDSA/SHA-384, EdDSA).

RFC 9575 states plainly that existing FAA regulations and standards for Remote ID "do not address trust," and that trust is a requirement for the parties with a stake in safe National Airspace System operation.

Read that again in the context of what you proposed. **The token, the org-and-person hierarchy, the endorsement chain, the anti-replay proof of possession — all of it is written, standardized, and sitting on the shelf. It is not mandated anywhere.** The gap between your concept and reality is not invention. It is adoption.

One honest limit, stated by the standard itself: DRIP proves *who signed*, not *whether the content is true*. An authenticated drone can still lie about its position. RFC 9575 explicitly requires observers to cross-check against physical-world observation and reject data that doesn't correlate, "as if signature validation failed." That means layer 4 — sensor-versus-claim correlation — is mandatory, not optional. You cannot build a trustworthy sky from radio attestation alone.

The network layer is partially built

The FAA operates **UAS Traffic Management (UTM)**, a set of services separate from but complementary to air traffic control, delivered by third-party **UAS Service Suppliers** ([FAA UTM program, statutory definition under P.L. 115-254 Sec. 376](#)). The FAA has also contracted trials to aggregate Broadcast Remote ID and convert it to **Network Remote ID** shared across the USS network ([Unmanned Airspace reporting on the ANRA trial](#)). This is your distribution backbone. It exists in prototype form.

The response layer expanded dramatically in the last eight months

This is the part most people don't know yet, and it matters enormously for your concept.

Counter-drone authority sits in **6 U.S.C. §124n**, from the Preventing Emerging Threats Act of 2018, which lets DOJ and DHS detect, identify, monitor, track, warn, disrupt, seize, disable, damage, or destroy drones threatening "covered facilities and assets" — and shields them from statutes that would otherwise make that illegal, including the Wiretap Act, the Computer Fraud and Abuse Act, and the Aircraft Sabotage and Aircraft Piracy Acts. DoD has parallel authority at **10 U.S.C. §130i** ([CRS report on low, slow, small UAS](#)).

Then, per the Congressional Research Service:

- The **FY2026 NDAA (P.L. 119-60)** extended §124n authority to **September 30, 2031**, broadened it to actions "necessary to enforce the law, protect the public, or to mitigate a credible threat,"

and for the first time **granted state, local, Tribal, and territorial law enforcement and correctional agencies** mitigation authority, contingent on DOJ training and certification.

- The enabling provision is the **SAFER SKIES Act**, enacted December 2025 as part of that NDAA. DOJ and DHS published an **Interim Final Rule on July 6, 2026, legally effective July 1, 2026**, with comments due September 4, 2026 ([Crowell client alert](#), [Homeland Security Today](#)).
- It creates **two tiers**. Tier 1 (detect, identify, monitor, track, warn) requires only an online certification. Tier 2 (disrupt, seize, take control, use reasonable force) requires hands-on training at the FBI's **National Counter-UAS Training Center**, the only authorized certifying body. Tier 1 personnel may not take Tier 2 action even in an emergency. Protected targets include people, facilities, assets, major events, critical infrastructure, and correctional facilities.

Separately, the FAA proposed a new **14 CFR Part 74** in May 2026 creating an **Unmanned Aircraft Flight Restriction** designation, letting critical-infrastructure owners petition to restrict drone flights over their sites — chemical, communications, dams, defense industrial base, energy, and more ([FAA fact sheet](#), [FAA newsroom](#), [Greenberg Traurig alert](#)).

And the policy tailwind is explicit: **Executive Order 14307, "Unleashing American Drone Dominance"** (June 6, 2025) directs agencies to accelerate integration of drones into the National Airspace System and reduce reliance on foreign-manufactured aircraft.

The threat driver is documented too. NORAD's commander reported **hundreds of drone incursions over U.S. military installations**, saying the Pentagon needs more technology and expanded authority to handle the volume ([DefenseScoop](#)). The UK recorded **266 incidents near defence facilities in 2025, roughly double the prior year** ([Reuters](#)).

So what is actually missing

Strip it down. Five gaps, in order of difficulty.

1. No mandated cryptographic authentication. Part 89 requires broadcast; it does not require signatures. DRIP exists but no rule points to it. This is the single highest-leverage change in the entire concept, and it is a rulemaking, not an invention.

2. No national root of trust or PKI hierarchy. Your "org and people and whatever" instinct is right — DRIP's hierarchical model needs registries, endorsement chains, revocation, and a defined root. Who holds the root? FAA? A federated set of registries under FAA oversight? That is a governance fight, not an engineering one.

3. The retrofit problem. Millions of aircraft are already flying with unsigned Remote ID. Signing requires key storage and compute on the aircraft or in a broadcast module. Bluetooth 4.x/5.x

message budgets are tight, which is precisely why RFC 9575 needed a specialized wire format. A hard cutover date orphans a large legacy fleet.

4. Government and military aircraft. You said federal and government drones should carry tokens too — including their own class of token. Correct instinct, hardest politics. DoD will not publish signing keys that let anyone geolocate sensitive operations. The workable design is a **separate hierarchy**: government aircraft carry valid tokens that resolve to "authorized, restricted attribution" for public observers while remaining fully attributable to cleared authorities. That preserves your rule — every aircraft is accountable to *someone* — without exposing operations.

5. Identity is not wired to interception. Today, counter-drone systems decide what to engage using radar signatures, RF emissions, and human judgment. None of them consume a cryptographic attestation feed, because none exists. The whole efficiency gain of Clean Sky — launch on *unattested*, ignore *attested* — requires a bus between layer 2 and layer 5 that nobody has built. This is the integration work, and it is the part you could realistically prototype.

Note what is **no longer** on this list: the takedown trigger. Capture-and-forfeit removes that problem, for the reasons below.

Capture, don't destroy — and this is the strongest part of the design

Map first, capture second, never shoot. That single choice resolves the hardest objection to the entire concept, and it turns out both the law and the hardware are already there.

The statute already authorizes exactly this

6 U.S.C. §124n(b)(1) lists the authorized actions in escalating order. Read them against your design:

PROVISION	AUTHORIZED ACTION	YOUR LAYER
(b)(1)(A)	"detect, identify, monitor, and track" the aircraft, without prior consent	Map
(b)(1)(B)	"Warn the operator... including through the use of remote identification broadcast"	Warn
(b)(1)(C)	"Disrupt control" of the aircraft	(skip)
(b)(1)(D)	"Seize or exercise control of " the aircraft	Capture
(b)(1)(E)	"Seize or otherwise confiscate" the aircraft	It becomes our property
(b)(1)(F)	"Use reasonable force, if necessary, to disable, damage, or destroy"	Never needed

That is your doctrine written into federal law, almost line for line. Map under (A), capture under (D), take title under (E), and **never touch (F)**. Note also that (B) explicitly contemplates warning the operator *through the Remote ID broadcast channel itself* — which means an authenticated Clean Sky link is already the statutorily-blessed way to say "you are unattested, land now" before anything else happens.

And because you stop at (E) rather than (F), the authority stays available to state and local agencies under the SAFER SKIES framework: seizure and control are Tier 2 actions requiring FBI certification, but they are squarely within what a certified local agency may do to protect people, venues, critical infrastructure, and correctional facilities.

The interceptor already exists and has 4,500 captures

The **Fortem DroneHunter F700** is a fully autonomous, radar-guided interceptor drone that does not jam and does not spoof — it pursues, fires an expanding tethered net, and tows the capture to a forensics recovery point ([UAS Feed](#), [Fortem Technologies](#)). As of early 2026:

- **More than 4,500 drone captures** across deployments on three continents, with operational validation in Ukraine, the Middle East, and East Asia.
- **85% first-shot capture rate**; a second shot is usually ready to follow.
- Reaches **50 mph within seconds of launch**, reloads in **under three minutes**, operates day and night in rain, snow, and fog.
- Guided by an **onboard AESA radar** (TrueView R20) that handles detection, tracking, and terminal engagement **with no ground-based cue required**.
- Has captured platforms larger than itself, including the Orlan-10 ISR drone and the Shahed-136 loitering munition.
- Engages at a stand-off of **3—10× the distance of ground-based mitigation**, so the capture happens far from the protected site.

Its autonomous modes map directly onto your sequence: **Pursue** (optical investigation before committing), **Attack** (fire net, begin tether tow toward a forensics staging area), **Defense** (entanglement against faster or larger threats), and **Tow-Away** (transport the airframe to a recovery point for exploitation). Small and medium tether nets tow Group-1 quadcopters home intact; the **DrogueNet** puts larger Group-2 aircraft under a parachute for a slow, predictable, controlled landing rather than a ballistic drop — with time to clear the ground below.

This is not a single-vendor bet, either. Net interception is a maturing category: **ParaZero** **DefendAir** received a follow-on order in July 2026 for non-explosive net-based interception protecting critical infrastructure ([The Defense Post](#)) and is being integrated into XTEND interceptor

drones in the thousands ([TechTime](#)), while **ARGUS Interception's A1-Falke** is adding lidar for terminal precision ([Unmanned Systems Technology](#)).

Why capture beats every alternative — including jamming

This is the argument that wins the room, and it has nothing to do with squeamishness about shooting things down.

Jamming is already obsolete against the threat that matters. A drone flying a GPS-waypoint mission carries its profile onboard and transmits nothing. There is no pilot datalink to sever, no uplink to overpower, no signal to intercept — and a jammer that cannot find a signal cannot stop the drone. Both sides in Ukraine adapted commercial drones to fly RF-silent for exactly this reason ([UAS Feed](#)). RF takeover is worse: it assumes a known command protocol *and* a live command link. Fiber-tethered drones defeat both.

Net capture is spectrum-independent and works on autonomous aircraft. The net physically entangles the airframe, a propeller catches the mesh, motors stall under load, and lift is lost. It is non-explosive, requires no spectrum authority, and is effective against autonomous, fiber-tethered, and swarming systems. Where jamming is unavailable, restricted, or ineffective, nets are described as the only non-kinetic option that physically removes the airframe from the airspace ([Netlaunchers technical guide](#)).

Live fire is a non-starter where you actually need this. Over a stadium, an airport approach, or a prison yard, kinetic rounds are rarely an option, and destroyed aircraft rain debris on the people you are protecting.

And capture is the only effect that preserves evidence. A netted airframe arrives intact, with SD cards, flight logs, and payload available for exploitation — the only interdiction method that delivers the aircraft whole when forensics and chain of custody matter ([Netlaunchers](#)). A destroyed drone tells you almost nothing. A recovered one tells you the operator, the launch point, the route, the target, the payload, and — if it is part of a coordinated effort — the rest of the network.

The compounding insight

Here is why your version is better than the kinetic version on its own terms, not just morally.

Shooting a drone down ends one incident. Capturing it **starts an investigation**. Every recovered airframe is a forensic sample that feeds attribution: who built it, who bought it, who launched it, what it was looking for. Do that a hundred times and you are no longer defending airspace incident-by-incident — you are mapping an adversary's entire program. That is a counterintelligence capability disguised as an air defense system, and it is the argument that gets it funded.

Destruction also destroys deterrence, because deterrence requires the adversary to believe they will be *identified*. A drone that disappears in a fireball is deniable. A drone sitting in an FBI evidence locker with its flight log intact is not.

The mapping layer that makes it work

"Map them immediately" is the load-bearing step, and it needs sensor fusion — no single modality is sufficient. The EU Joint Research Centre's technical assessments of counter-drone detection, tracking, and identification stress that acoustic, electro-optical, radar, and RF sensors each have distinct strengths and limits, and that **multi-sensor data fusion is what makes real-time identification robust** ([JRC on C-UAS detection and identification](#), [JRC on counter-drone data fusion](#)).

Clean Sky adds a fifth modality that changes the math: **cryptographic attestation as a sensor input**. Fuse radar, RF, EO/IR, and acoustic tracks into a single airspace picture, then subtract every contact that can prove itself. What remains is your target set — small, prioritized, and defensible. This is the set-difference architecture, and it is what lets a handful of interceptors cover a large area, because they are not chasing everything that flies. They are chasing only what will not identify itself.

Layer 6 — The Sovereign Fleet

This is the part that does not exist anywhere, and it is where your program stops being a synthesis of other people's work and becomes yours.

The idea: our interceptors are not just nets on rotors. Each one is an **encrypted, air-gapped flying forensic node**. It carries its own attested identity, talks only to its own fleet over a closed encrypted mesh, and begins documenting the target the moment it launches — so by the time the net fires, we already have a forensic profile of the intruder. The capture confirms what the fleet has already mapped.

Our own drones are attested first

Every interceptor carries its own DRIP Entity Tag in a hardware secure element, issued under the government hierarchy. This matters more than it sounds. It answers "who watches the watchers," it means our own fleet is subject to the same rule we are imposing on everyone else, and it makes a stolen or cloned interceptor immediately detectable — a captured Sovereign Fleet airframe cannot be flown against us, because its key cannot be extracted and its revocation propagates through the mesh.

Air-gapped means unjammable and unhijackable

The fleet has **no external command-and-control dependency in flight**. This is not paranoia — it is the direct lesson of the interception hardware that already works. The DroneHunter F700's onboard AESA radar handles detection, tracking, and terminal engagement **with no ground-based cue required** ([UAS Feed](#)). Extend that principle to the whole system: if there is no uplink, there is no uplink to jam, spoof, or take over. An adversary who has just learned that our drones are coming cannot cut the cord, because there is no cord.

The mesh is *inside* the air gap. Interceptors coordinate with each other over an authenticated, encrypted mobile ad-hoc network with pre-provisioned rotating keys — a closed enclave that happens to be moving. This is an active research area with known tradeoffs: MANET and delay-tolerant approaches give adaptability in dynamic settings but face latency and connection-stability challenges, while Wi-Fi mesh gives better coverage and stability at an energy cost that must be optimized for autonomous operation ([Premier Science, drone swarm to ground-base transmission](#)). Design accordingly: assume intermittent links, make every node able to complete its mission alone, and treat mesh consensus as an enhancement rather than a requirement.

The flying forensic lab

Each interceptor collects, before and during capture:

COLLECTION	WHAT IT YIELDS
RF fingerprint (raw I/Q)	Hardware-level identity of the transmitter, independent of any claimed ID
Control-link characterization	Protocol, hopping pattern, whether the aircraft is RF-silent and autonomous
EO/IR imagery	Airframe type, payload, modifications, markings
Acoustic signature	Motor and propeller class, useful when RF is absent
Kinematic track	Launch bearing, route, loiter points, target dwell
Attestation transcript	Exactly how and when identity verification failed — the legal predicate

The RF fingerprint is the load-bearing one, and it is real science, not aspiration. Fingerprinting works by extracting nuanced but sufficiently detailed characteristics from a received signal ([arXiv, generic ML framework for RF fingerprinting](#)). Ensemble-learning models such as **DrIfTeR** detect, identify, and classify drones purely from RF fingerprints ([ScienceDirect](#)), wavelet-transform analytics have been benchmarked for RF-based UAV detection and identification ([arXiv](#)), and domain-invariant approaches like **CrossRF** are specifically attacking the generalization problem that has held fingerprinting back ([arXiv](#)). There is even prior art for the inverse — **AirID** deliberately

injects a custom RF signature into transmitted I/Q samples to mark authorized UAVs ([IEEE GLOBECOM](#)) — which is a hardware-layer complement to cryptographic attestation.

Why this is a genuine advance: a cryptographic token can be absent, but an RF fingerprint cannot be. A drone that refuses to identify itself still radiates a hardware signature. Pair attestation (what it *claims*) with fingerprinting (what its transmitter *is*) and you can recognize the same physical airframe across separate incidents, weeks apart, even if it never broadcasts a valid token once. That is what turns individual captures into a case file.

Evidence egress — all three tiers, selected by mission

You asked for all of it, and the honest answer is that all three belong, at different classification levels. What you cannot have is one drone that is simultaneously air-gapped and streaming to Azure. What you can have is a fleet with three configurations:

Tier A — Sovereign local (default). Fully air-gapped end to end. Onboard encrypted vault, mesh-only coordination, recovery to an on-premise forensic lab. No cloud dependency of any kind. This is the configuration for contested environments and the one that matches your local-first posture.

Tier B — One-way sync to a forensic enclave (recommended for scale). After recovery, evidence crosses a **data diode** into an Azure confidential-computing enclave. A data diode is a hardware device that enforces unidirectional flow at the physical layer — the hardware is *incapable* of bidirectional transmission, so data can be pulled out of an air-gapped system with no return pathway and no possibility of reverse communication ([Owl Cyber Defense](#), [Nexor](#)). NATO documents single-fiber diode designs for exactly this purpose — one-way transfer without compromising the confidentiality or integrity of the air-gapped network ([NATO Information Assurance](#)).

The destination side is available at government classification levels today: Azure Confidential Computing reached general availability on AMD SEV-SNP virtual machines **across all U.S. government data classification levels** ([Microsoft Azure Government blog](#)), and confidential computing hardens the environment against the host, the hypervisor, the host administrator, and even your own VM administrator ([Microsoft Learn](#)). Microsoft Sovereign Cloud adds data-residency and operational-sovereignty controls designed for governments and regulated industries ([Microsoft Learn](#)). So the "Azure layers of cyber forensics" instinct is sound — it just belongs on the far side of a diode, not on the airframe.

Tier C — Live encrypted uplink (optional, degraded). Real-time streaming to the enclave during flight. Faster analysis and remote human review, at the cost of a jammable, detectable, attackable dependency. Worth having for permissive environments like a stadium perimeter. Never the default, and the fleet must fall back to Tier A the instant the link degrades.

Pattern-of-targeting analysis

This is the capability you were reaching for with "check patterns of targeting certain individuals or areas," and it is the most operationally valuable thing in the whole program — because it addresses a harm that is already happening and already prosecutable.

Drone harassment and stalking are crimes under existing law, and local stalking, trespass, and harassment statutes have already secured convictions without waiting on the FAA ([DRONERESPONDERS](#)). In Rockingham County, Virginia, a man was charged with two counts of spying using an electronic device, four counts of entering a property to harass using a drone, and two counts of stalking with fear of death or assault ([Police1](#)). Practitioners note there is no single drone law for this — ordinary trespass, voyeurism, harassment, stalking, and criminal-damage statutes get applied to drone facts, and **the civil/criminal line generally turns on intent and repetition** ([Watkins, drone privacy and criminal misuse law](#)).

Read that last clause again: **intent and repetition**. Repetition is a data problem, and it is the exact data the Sovereign Fleet produces. A single overflight is ambiguous. Nine overflights of the same residence at the same hour across three weeks, tied to one RF fingerprint, is a stalking case with the element of repetition already proven. Today victims cannot establish that pattern because nobody is recording it. Sovereign Clean Sky records it by default.

What the analysis layer does:

- **Fingerprint persistence** — link separate incidents to the same physical airframe via RF signature, even with no valid token.
- **Repetition detection** — flag recurring overflights of the same location, and cluster by time of day and day of week.
- **Dwell and behavior classification** — distinguish transit from loiter, and loiter from directed observation of a specific structure.
- **Launch-point regression** — back-track kinematic tracks across incidents to converge on an operator's staging area.
- **Campaign linking** — connect incidents that share fingerprints, hardware, or launch geometry into a single case, whether the target is a person or a substation.
- **Evidence packaging** — emit a sealed, hash-chained package per incident and per campaign: attestation failure proof, fused sensor track, fingerprint match, intercept log, custody record.

And here is the guardrail, stated plainly, because this is the part that will decide whether the program is credible. The analysis profiles *drone behavior*, not residents. It must not become a standing database of who lives near what. The design constraint is that a targeting analysis for a private individual is opened on that individual's complaint or consent, or under a protective order

— never as ambient monitoring of a neighborhood. Aggregate pattern analysis runs against protected facilities and critical infrastructure, which have institutional standing to consent. Build it the other way and you have created the surveillance system your own project family exists to argue against, and it will be attacked on exactly those grounds. Victim-initiated, consent-scoped, and audit-logged is both the ethical design and the survivable one.

Honest engineering constraints

- **Size, weight, and power.** A small interceptor cannot carry a full forensic lab. Realistic split: lightweight onboard capture (wideband RF snapshot, EO/IR, kinematics) with heavy analysis — fingerprint model inference, campaign linking — running in the ground enclave. Do not promise onboard deep learning at scale.
- **Fingerprint generalization is unsolved.** RF fingerprinting degrades across channel conditions and hardware batches; that is precisely the problem CrossRF and similar work target. Treat fingerprint matches as investigative leads with confidence scores, never as courtroom-grade identity on their own.
- **Air gap costs latency.** Tier A means evidence is hours old by the time it reaches an analyst. That is the correct trade in a contested environment and the wrong one at a stadium. Make the tier a mission parameter, not a build-time decision.
- **Key management is the real program risk.** Hardware secure elements, provisioning, rotation, revocation propagation across an intermittently connected mesh, and recovery when an interceptor is lost. This is where sovereign systems usually fail, and it deserves more design attention than the airframe.

The reframe that makes this fundable

Your strongest argument is not "shoot down unregistered drones." It is this:

Today, a hostile drone hides inside the noise of an unauthenticated sky. Mandate cryptographic attestation and the noise disappears. Every legitimate aircraft becomes provable, so every illegitimate one becomes *conspicuous*. Detection stops being a needle-in-haystack sensor problem and becomes a set-difference problem: what the sensors see, minus what can prove itself.

That is a genuinely powerful shift. It converts an intractable detection challenge into a tractable verification challenge, and it makes the response layer proportionate because you finally know who is who.

And the second half of the pitch is what makes it politically survivable: **nothing gets shot down**. Unattested aircraft are netted, towed home intact, and forfeited as evidence. No debris, no spectrum interference, no dead hobbyist drone falling on a school, no deniability for the adversary. The reason it deters is not force — it is that **anonymity ends and the airframe ends up in an evidence locker**.

What you could actually build

You don't need federal authority to build the proof. The standards are public and the crypto is implementable. A credible prototype, in ascending order:

1. **DET issuance authority** — a local-first registry that mints RFC 9374 DRIP Entity Tags for simulated operators, organizations, and aircraft, with an endorsement chain and revocation list. This is the piece that maps directly to work you've already done on cryptographic custody and evidence integrity.
2. **Signing aircraft simulator** — emit ASTM F3411-style Remote ID messages plus RFC 9575 Authentication Messages with real signatures, over Bluetooth or Wi-Fi beacons.
3. **Observer / verifier** — receive broadcasts, validate signature chains, and classify each contact as *attested*, *unattested*, *expired*, *revoked*, or *spoof-suspected*.
4. **Adversary harness** — run the public spoofer against your own verifier to demonstrate that unsigned Remote ID fails and signed Remote ID holds. **This is the demo that convinces people**. Side-by-side: today's rule collapses, DRIP survives.
5. **Correlation layer** — feed in a synthetic sensor track and show detection of a drone whose signed position claim disagrees with observed position, per RFC 9575's mandatory non-cryptographic validation.
6. **Airspace picture** — a clean-sky dashboard where attested traffic renders normally and everything else escalates, with an immutable evidence log suitable for prosecution.
7. **Intercept tasking simulator** — the layer-2-to-layer-5 bus that does not exist anywhere. Given a fused track list, automatically classify each contact, apply the escalation ladder (attest → warn over the RID channel → task interceptor → capture → tow to recovery → open custody record), and show interceptor assignment against multiple simultaneous unattested contacts. This is the piece that makes the whole doctrine legible in one screen.
8. **Chain-of-custody record** — for each capture, a sealed evidence package: attestation failure proof, fused sensor track, intercept log, recovery point, and hash chain. This is the same cryptographic custody pattern you have already built elsewhere, pointed at a captured airframe instead of a ballot.

Steps 1 through 4 are achievable on your own hardware with no special permissions. Step 4 alone is a compelling artifact for a policy audience, and steps 7–8 are where your existing custody-and-evidence work becomes a genuine differentiator.

Straight assessment

The idea is sound, the diagnosis is accurate, and you arrived independently at a gap that aviation-security researchers and an IETF working group have been documenting for years. That is worth taking seriously.

What it is not is novel invention — DRIP already specifies the token layer, and pretending otherwise would weaken any pitch you make. Your contribution is the **synthesis and the posture**: mandate universal attestation across civil *and* government fleets, wire it to the newly expanded SAFER SKIES response layer, and adopt clean-sky-by-default as national policy. Nobody has assembled those pieces into one program.

The capture-and-forfeit refinement materially strengthens it. It is not a softening — it is the version that is legally cleaner (§124n(b)(1)(D) and (E) rather than (F)), operationally superior against RF-silent autonomous drones, usable over populated ground where the threat actually is, and intelligence-generating rather than intelligence-destroying. It also keeps state and local agencies in play under SAFER SKIES.

What remains unresolved is the government-fleet carve-out. DoD will not publish keys that let anyone geolocate sensitive operations, and "every drone including federal ones" is the provision most likely to be stripped in markup. The workable answer is a separate hierarchy with restricted attribution — valid token, resolvable only by cleared authorities. Get that right and this is a serious proposal.

One caution worth carrying into any pitch: a mandatory national attestation registry covering every drone and operator is a large, sensitive identity database, and the privacy objection will arrive immediately. The Session ID precedent in the existing Remote ID rule is your best answer — public observers see a rotating pseudonym, authorities resolve identity only through the registry, and the July 2026 SAFER SKIES rule already includes privacy safeguards and reporting requirements you can build on rather than reinvent.

Sources

- FAA, Remote ID getting started — https://www.faa.gov/uas/getting_started/remote_id

- 14 CFR Part 89, eCFR — <https://www.ecfr.gov/current/title-14/chapter-I/subchapter-F/part-89>
- FAA, Remote ID Final Rule (PDF) — https://www.faa.gov/sites/faa.gov/files/2021-08/RemoteID_Final_Rule.pdf
- FAA, Remote ID talking points — <https://www.faasafety.gov/files/gslac/library/documents/2023/Aug/388879/Remote%20ID%20Talking%20Points%20FINAL%20v2.1.pdf>
- RFC 9153, DRIP Requirements and Terminology — <https://datatracker.ietf.org/doc/rfc9153/>
- RFC 9374, DRIP Entity Tag (DET) — <https://www.rfc-editor.org/info/rfc9374/>
- RFC 9575, DET Authentication Formats and Protocols for Broadcast RID — <https://datatracker.ietf.org/doc/rfc9575/>
- RFC 9886, DRIP Registries — <https://datatracker.ietf.org/doc/rfc9886/>
- IETF DRIP working group charter — <https://datatracker.ietf.org/group/drip/about/>
- IANA DRIP assignments — <https://www.iana.org/assignments/drip/drip.xml>
- TBRD: Tesla Authenticated Broadcast Remote ID, arXiv — <https://arxiv.org/html/2510.11343v2>
- Exploration of Remote ID Vulnerabilities, Linköping University — <https://liu.diva-portal.org/smash/get/diva2:2073639/FULLTEXT01.pdf>
- Security of ADS-B and Remote ID Systems, PMC — <https://pmc.ncbi.nlm.nih.gov/articles/PMC12846276/>
- Drone Remote ID Spoofer, Cyber-Defence Campus — <https://github.com/cyber-defence-campus/droneRemoteIDSpoofer>
- 6 U.S.C. §124n, authorized counter-UAS actions (Cornell LII) — <https://www.law.cornell.edu/uscode/text/6/124n>
- CRS, Law Enforcement and the Evolving Counter-UAS Landscape — <https://www.congress.gov/crs-product/IN12661>
- CRS, Low, Slow, Small UAS — <https://www.congress.gov/crs-product/R48477>
- Crowell, SAFER SKIES Act Interim Final Rule — <https://www.crowell.com/en/insights/client-alerts/doj-and-dhs-issue-interim-final-rule-on-state-and-local-counter-drone-authority-under-the-safer-skies-act>
- Homeland Security Today, new federal counter-drone rule — <https://www.hstoday.us/subject-matter-areas/unmanned-vehicles/new-federal-counter-drone-rule-gives-local-police-and-corrections-agencies-authority-to-detect-disable-dangerous-drones/>
- Executive Order 14307, Unleashing American Drone Dominance — <https://www.whitehouse.gov/presidential-actions/2025/06/unleashing-american-drone-dominance/>

- FAA, Restricting Drones Near Critical Infrastructure Sites — <https://www.faa.gov/newsroom/restricting-drones-near-critical-infrastructure-sites>
- FAA fact sheet, critical infrastructure restrictions (PDF) — <https://www.faa.gov/newsroom/fact-sheets/2026-Restricting-Drones-Critical-Infrastructure.pdf>
- Greenberg Traurig, proposed Part 74 alert — https://www.gtlaw.com/-/media/files/insights/alerts/2026/05/gt-alert_faa-proposes-new-process-for-restricting-drone-flights-over-critical-infrastructure.pdf
- FAA, UAS Traffic Management — https://www.faa.gov/uas/advanced_operations/traffic_management
- FAA, UTM statutory definitions, P.L. 115-254 Sec. 376 — https://www.faa.gov/sites/faa.gov/files/PL_115-254_Sec376_UAS_Traffic_Management.pdf
- Unmanned Airspace, Network Remote ID trial — <https://www.unmannedairspace.info/uncategorized/anra-and-partners-win-faa-contract-to-trial-network-remote-id-messaging/>
- DefenseScoop, NORAD on drone incursions over U.S. bases — <https://defensescoop.com/2025/02/13/drone-incursions-us-military-bases-norad-northcom-counter-small-uas/>
- Reuters, UK military base drone incidents doubled — <https://www.reuters.com/world/uk/drone-incidents-uk-military-bases-doubled-last-year-2026-02-02/>

Capture and interception

- Fortem Technologies, DroneHunter F700 — <https://www.fortemtech.com/products/dronehunter-f700/>
- UAS Feed, Fortem DroneHunter explained — <https://uasfeed.com/article/fortem-dronehunter-explained>
- Battle Policy, DroneHunter F700 reusable net-capture interceptor — <https://www.battlepolicy.com/fortem-dronehunter-f700/>
- National Defense Magazine, Hunting Drones With Drones — <https://www.nationaldefensemagazine.org/articles/2023/10/26/hunting-drones-with-drones>
- Netlaunchers, Counter-Drone Net Systems technical guide — <https://netlaunchers.com/guides/counter-drone-net-systems>
- The Defense Post, ParaZero DefendAir counter-drone order — <https://thedefensepost.com/2026/07/27/parazero-new-defendair-order/>
- TechTime, ParaZero and XTEND interceptor partnership — <https://techtime.news/2026/04/05/parazero-deepens-defense-shift-with-xtend-partnership/>

- Unmanned Systems Technology, lidar for net-based interceptors — <https://www.unmannedsystemstechnology.com/2026/05/digital-lidar-to-enhance-counter-drone-intercept-systems/>
- Norsk Luftvern, Soft Kill: Non-Kinetic Counter-Drone Systems — <https://norskluftvern.com/2026/03/23/soft-kill-non-kinetic-counter-drone-systems/>

Forensics, air-gap, and pattern analysis

- arXiv, Generic ML framework for RF fingerprinting — <https://arxiv.org/html/2510.09775v3>
- ScienceDirect, DrlfTeR drone RF fingerprinting — <https://www.sciencedirect.com/science/article/abs/pii/S2666281725000873>
- arXiv, CrossRF domain-invariant RF fingerprinting — <https://arxiv.org/abs/2505.18200>
- arXiv, Wavelet transform analytics for RF-based UAV ID — <https://arxiv.org/abs/2102.11894>
- IEEE GLOBECOM, AirID injected RF fingerprints — <https://dl.acm.org/doi/10.1109/GLOBECOM42002.2020.9322561>
- Owl Cyber Defense, one-way data diodes — <https://owlcyberdefense.com/learn-about-commercial-data-diodes/>
- Nexor, data diode unidirectional transfer — <https://www.nexor.com/data-diode>
- NATO Information Assurance, Arbit 10GbE data diode — <https://www.ia.nato.int/DocumentGenerator/repository/version/03b28133-895c-4764-8177-4dc4049ead21/Arbit-Data-Diode-10GbE>
- Microsoft Azure Government, Confidential Computing GA across US gov classification levels — <https://devblogs.microsoft.com/azuregov/azure-confidential-computing-for-us-gov/>
- Microsoft Learn, Azure Confidential Computing scenarios — <https://learn.microsoft.com/en-us/azure/confidential-computing/use-cases-scenarios>
- Microsoft Learn, Microsoft Sovereign Cloud — <https://learn.microsoft.com/en-us/azure/azure-sovereign-clouds/microsoft-sovereign-cloud>
- Premier Science, drone swarm to ground-base data transmission — <https://premierscience.com/pjs-25-1302/>
- DRONERESPONDERS, when a drone becomes a weapon of harassment — <https://www.droneresponders.org/post/when-a-drone-becomes-a-weapon-of-harassment>
- Police1, Rockingham County drone stalking case — <https://www.police1.com/drones/what-happens-when-a-drone-stalks-you-at-first-nothing-but-a-va-woman-found-a-way-to-fight-back>
- Watkins, drone privacy, trespass and criminal misuse law — <https://www.jaredwatkins.com/research/drone-detection/privacy-trespass-and-misuse-law/>

Detection and sensor fusion

- EU JRC, C-UAS detection, tracking and identification technology — <https://publications.jrc.ec.europa.eu/repository/handle/JRC140692>
- EU JRC, Counter-drone systems and data fusion (PDF) — https://publications.jrc.ec.europa.eu/repository/bitstream/JRC139587/JRC139587_01.pdf
- Quickset, How Counter-UAS Systems Work — <https://www.quickset.com/how-counter-uas-systems-work/>

BORN BETWEEN GENERALS, LLC • Brandon, Florida • cleansky.bornbetween2generals.com

Unclassified public policy proposal by a private company. Not a government publication; carries no federal endorsement, seal, or authority.