

BORN BETWEEN GENERALS, LLC

OPERATION ANGELS · BB2G SOLUTIONS

BRANDON, FLORIDA

AUGUST 30, 2026

UNCLASSIFIED

The President of the United States
The White House
1600 Pennsylvania Avenue NW
Washington, DC 20500

RE: SOVEREIGN CLEAN SKY — CLOSING THE AUTHENTICATION GAP IN AMERICAN AIRSPACE

Mr. President,

Every drone flying legally over the United States is already required to announce who it is. Almost none of them can prove it. The Remote ID broadcast mandated under 14 CFR Part 89 is unauthenticated plain text — a license plate anyone can print. Working spoofers are published openly and run on hardware that costs less than dinner. This means that on the most basic question we can ask about an aircraft over a military installation, a substation, a stadium, or a family's back yard — **who are you** — our answer today is an unverified assertion from the aircraft itself.

I am not writing to report a gap you have not already acted on. Your Executive Order on *Unleashing American Drone Dominance* pushed this industry forward, and the SAFER SKIES Act extended counter-drone authority through September 30, 2031 and put it, for the first time, in the hands of state and local law enforcement. The authority exists. The industry exists. What is missing is the one layer that makes both of them mean something: **proof**.

The remedy is already written. The Internet Engineering Task Force has published the standard that makes Remote ID trustworthy — an identifier that is itself a public-key commitment, and an authentication message in which the aircraft proves it holds the private key by signing unpredictable data. It is Standards Track. It is finished. It is mandated nowhere. **The gap is not invention. It is adoption.**

And adoption changes the shape of the problem, not just its difficulty. Today we ask sensors to find one hostile drone inside a sky full of anonymous ones — a needle in a haystack, and the haystack grows every year. Require attestation and that becomes simple subtraction: what the sensors see, minus what can prove itself. Whatever is left is the entire target list. **A clean, attributable sky makes an unattributable aircraft conspicuous.** That is the whole idea, and it is why this is infrastructure rather than equipment.

On what happens next, I want to be equally plain, because I believe the current instinct is wrong. We should not shoot these aircraft down. Federal law already authorizes us to *seize or exercise control* and to *seize or otherwise confiscate* — capture and forfeiture — before it ever reaches the use of force. Net-capture interceptors have completed thousands of recoveries across three continents. A drone brought down under a net arrives intact, with its flight log, its payload, and its launch point still readable. A drone destroyed in the air arrives as debris and a deniable incident.

Deterrence does not come from the fireball. It comes from the end of anonymity, plus a recovered airframe sitting in an evidence locker. Do that a hundred times and we are no longer defending airspace one incident at a time — we are mapping an adversary's entire program, and we are doing it with evidence that survives a courtroom.

There is one more thing I would ask you to look at, because it is the part nobody is building. Our own interceptors should be encrypted, air-gapped, and attested under the government's own hierarchy — no uplink to jam, no cord to cut, no stolen airframe worth stealing — and they should fly as forensic instruments, not just as nets. They can capture a transmitter's hardware fingerprint, which cannot be forged the way a token can be forged and cannot be withheld the way a token can be withheld. That single capability lets us recognize the same physical aircraft across separate incidents weeks apart, which is how a series of overflights becomes a provable pattern instead of a string of unrelated complaints.

That matters far from any military fence line. In Virginia, a woman was followed over her own property by a drone for months before charges were finally brought. The law she needed already existed; what she did not have was a record. The line between a nuisance and a crime usually turns on intent and repetition, and **repetition is a data problem we are simply not solving**. Built correctly — victim-initiated, consent-scoped, audit-logged, profiling drone behavior and never residents — this is the difference between telling that woman we are sorry and handing her a case.

Accordingly, I respectfully ask for five things:

1. **Direct the FAA to adopt the IETF DRIP standards as the authentication layer for Remote ID**, with a fixed compliance date and a published retrofit path for the existing fleet.
2. **Establish the federal attestation registry with privacy designed in** — rotating public pseudonyms on the existing Session ID model, with identity resolvable only through the registry by authorized parties.
3. **Create a separate attestation hierarchy for government and military aircraft** — a valid token with restricted attribution — rather than a carve-out that would hand adversaries a category to hide in.

4. **Make capture, not destruction, the default mitigation**, and fund the recovery and forensic intake that turns every intercepted airframe into evidence.
5. **Authorize a victim-initiated pattern-of-targeting evidence service**, so that repetition can be proven for a family and for a substation alike.

The first of those costs a rulemaking, not an appropriation, and it is the one that unlocks the other four. And you do not have to take any of this on faith. My company will build and publish the working proof at our own expense — an identity issuing authority, a signing aircraft, an independent verifier, and an adversary harness that runs the publicly available spoofer against the current unsigned rule and the authenticated one side by side. We will show one collapsing and the other holding. If it fails, we will publish that too.

I am a small business owner in Brandon, Florida, and I build proof-oriented systems because I believe institutions earn trust by making their claims verifiable rather than by asking to be believed. I am asking the United States to apply that same standard to its own sky. The authority is in hand and it expires in 2031. The standard is finished and waiting. What remains is a decision.

Thank you for your time and for your service to our country. I am at your disposal, and everything on the accompanying site — including every limitation of this proposal — is published in the open.

Respectfully,

KRISSY HALL

FOUNDER • BORN BETWEEN GENERALS, LLC
BRANDON, FLORIDA • [CLEANSKY.BORNBETWEEN2GENERALS.COM](https://cleansky.bornbetween2generals.com)

BORN BETWEEN GENERALS, LLC • BB2G Solutions • Brandon, Florida • cleansky.bornbetween2generals.com
Unclassified public policy proposal by a private company. Not a government publication; carries no federal endorsement, seal, or authority.
Full text, every cited source, and a published statement of limits: cleansky.bornbetween2generals.com