

POLICY BRIEFING

Unauthenticated Aviation VHF Voice Communication

Synthetic voice, correct phraseology, and the absence of cryptographic authentication on air traffic control frequencies

Prepared July 2026 · Sunny Paul Smith with Ernie Ortiz (retired air traffic controller, technical adviser)

Document URL: <https://haijacked.com/brief.pdf> · Evidence: <https://haijacked.com/evidence>

AVIATION VHF VOICE · 118.0–136.975 MHz · NO ENCRYPTION · NO SIGNATURE · NO CHALLENGE-RESPONSE

EXECUTIVE SUMMARY

Aviation air traffic control (ATC) voice communication is carried on unencrypted analog VHF channels. There is no cryptographic authentication of the speaker. Pilots comply with instructions based on recognition: the voice sounds like the controller, arrives on the expected frequency, uses correct phraseology, and is operationally plausible.¹⁴

That recognition-based model was adequate when unauthorized transmissions were limited to amateur impostors who betrayed themselves through incorrect phraseology. It is no longer adequate. In August 2025, a cloned-controller-voice demonstration was presented on the main track at DEF CON 33.²³ In April 2026, a peer-reviewed conference paper from George Washington University reported that synthetic ATC speech preserved safety-critical tokens (altitude, heading, runway, frequency) with a critical-token F1 of 0.958. Speaker-embedding cosine similarity was 0.726; the paper notes that same-speaker verification typically reaches ≥ 0.8 for the same utterance, so 0.726 across different utterances is the striking figure.⁴

Congress has appropriated and requested more than \$32 billion for ATC modernization, targeting completion by the end of 2028. The program modernizes radar and telecommunications infrastructure. It does not appear to authenticate the voice carried on the frequency.⁵

This briefing does not propose a specific technical remedy. It documents the gap and recommends that the question of voice authentication be asked on the record in any hearing touching FAA modernization or artificial intelligence in critical infrastructure.

1. The Vulnerability

Aviation VHF voice communication operates on unencrypted analog channels in the band 118.0–136.975 MHz. There is no cryptographic handshake, no digital signature, and no challenge-response mechanism on these channels.¹

In operational practice, a pilot complies with an instruction because four cues align: (1) the voice sounds like the controller; (2) it arrives on the expected frequency; (3) it uses correct phraseology; and (4) the instruction is contextually plausible. Authentication, in practice, is recognition.

The openness of the channel is deliberate and operationally valuable. Pilots need to hear other traffic, not only the controller. That “party line” property is why encryption has consistently been rejected for this layer. Any durable treatment of the authentication gap must reckon with that operational constraint; encryption of the open frequency is not assumed here as the answer.

2. Why Recognition No Longer Suffices

Two capabilities have changed the risk calculus.

Synthetic voice identity. Modern systems can clone a controller’s voice from publicly available recordings. Hobbyist websites archive thousands of hours of live controller audio, indexed by facility. Synthesis software is open source;

required hardware is commodity.

Accurate phraseology. Language models and ATC-oriented text-to-speech systems can generate correct radiotelephony — altitude, heading, runway assignment, frequency change — in the identity of a specific controller. The historical defense against impostors (incorrect phraseology and inability to answer a read-back) no longer applies with the same force.

2.1 Public demonstration — DEF CON 33 (August 2025)

On August 10, 2025, Andrew “Helicopters of DC” Logan — an audio engineer and aviation-transparency researcher — presented “Voice Cloning Air Traffic Control: Vulnerabilities at Runway Crossings” on the *main* DEF CON 33 speaker track (not the Aerospace Village). The presentation included a demonstration of using a cloned controller voice to instruct an aircraft to cross an active runway in front of landing traffic.² The talk was covered by *Aviation International News* on August 22, 2025.³ A recording of the talk is publicly available.⁶

2.2 Peer-reviewed research — IEEE ICNS 2026

Dao Vu and Peng Wei of George Washington University presented “Generating Realistic Air Traffic Control Voice Communication using AI-based Text-to-Speech Models,” a **peer-reviewed conference paper** (not a journal article), at IEEE ICNS 2026 — the 26th Integrated Communications, Navigation and Surveillance Conference — in Herndon, Virginia, April 14–16, 2026.⁴

The work was evaluated against 1,000 authentic controller utterances from the ATCOSIM corpus. Reported results included:

METRIC	RESULT	NOTES
Word error rate	3.9% (median 0%)	Compared to authentic ATCOSIM utterances
Critical-token F1	0.958	Altitude, heading, runway, frequency preserved
Speaker-embedding cosine similarity	0.726	Same-speaker verification typically ≥0.8 for same utterance; 0.726 across different utterances is the striking figure

The authors’ stated threat model, quoted verbatim:

“an adversary capable of generating synthetic ATC-style audio conditioned on publicly available recordings of controller speech... exploiting the absence of cryptographic authentication and encryption in legacy VHF voice communication architectures.”⁴

A finding of particular operational significance: prosody and cadence were the weakest-reproduced dimension — i.e., the remaining detection cue. The authors then listed as a limitation that evaluation was conducted “without explicit VHF channel modeling, radio compression artifacts, or environmental noise injection.”⁴ That limitation is named as future work in the research literature; it is precisely the class of gap an adversary would seek to close.

3. Historical Precedent — Correctly Framed

Unauthorized transmissions on ATC frequencies are a documented phenomenon. The following incidents are drawn from a single contemporaneous wire story (ABC News, August 29, 2000), which itself cites the Sunday Times for the East Midlands case; SKYbrary summarizes the same attack class.⁷⁸

DATE	INCIDENT
April 1999	USAir flight diverted on approach to Reagan National by an unknown voice on frequency.
December 1999	Transmitter stolen from Edinburgh Airport used to issue false commands.

1999	Ham radio operator issued false instructions at Manchester.
July 2000	Controller at East Midlands Airport transmitted “Respond to my voice only” after unauthorized transmissions.

These incidents are approximately twenty-six years old, and three of the four are British. They establish that the attack class is old. They establish nothing about present-day U.S. operational posture.

Regulators at the time assessed such incidents as low-severity because pilots read instructions back and impostors betrayed themselves with incorrect phraseology. An amateur with a transmitter could not sustain the performance. That is exactly the defense that has stopped working against a model trained on archived controller audio: it produces correct phraseology, in the identity of the specific controller who worked that position, and it can answer a read-back.

As far back as 2000, the FAA acknowledged that unauthorized people periodically use controller frequencies to issue false instructions, including “ghost transmissions” at JFK. Reporting at the time indicated that no capability existed to block or filter such broadcasts. We are not aware of any deployed since.⁷ *Note: a widely repeated line that “the FAA says no technology exists to block these broadcasts” originates as a reporter’s paraphrase in that 2000 article, not as a current agency statement. It is twenty-six years old and should not be read as the FAA’s present position.*

4. Modernization Funding and Staffing Context

4.1 Funding

\$12.5 billion was appropriated for ATC modernization in the reconciliation bill signed July 4, 2025. Approximately \$20 billion additional has been requested. The combined commitment is more than \$32 billion. The program targets completion by the end of 2028.⁵

Funds are directed at replacement of up to 612 legacy radar systems by June 2028; migration of legacy copper telecommunications to fiber, satellite, and wireless (approximately 40% complete at last reported status); and facility replacement. **None of these investments authenticates the voice carried on the frequency.** The program modernizes the transport layer while leaving the trust layer unchanged.

4.2 Staffing

The FAA entered 2026 approximately 3,544 certified controllers below its own staffing target. According to NATCA (National Air Traffic Controllers Association), more than 41% of certified controllers work 10-hour days, six days per week — a union figure, not FAA data, and attributed as such.⁹ On May 15, 2026, the FAA revised its staffing target downward from 14,633 to 12,563.

Fatigue degrades exactly the pattern-recognition capability that currently constitutes the only line of defense against a synthetic voice that sounds right and speaks correctly.

5. Legal Framework

Transmitting false instructions to aircraft is criminal under:

- 49 U.S.C. § 46308 — interference with air navigation (up to 5 years)
- 18 U.S.C. § 32, including § 32(a)(8) — knowingly communicating false information endangering an aircraft in flight (up to 20 years)
- 47 U.S.C. § 333 — willful or malicious interference with radio communications

Current federal synthetic-media legislation is directed elsewhere: TAKE IT DOWN Act (S.146, enacted May 19, 2025); AI Fraud Accountability Act of 2026 (S.3982, introduced March 4, 2026); NO FAKES Act of 2026 (S.4591, reported out of Senate Judiciary unanimously June 18, 2026).

Precision on the gap: Safety-critical operator impersonation is covered criminally *after the fact*. What is missing is that no federal synthetic-media statute reaches impersonation of a safety-critical operator as such, and the general aviation-interference statutes predate synthetic voice — they punish the act afterward while requiring no capability to detect or prevent it.

6. Scope — What This Briefing Does Not Claim

- We do not claim this attack has been carried out against civil aviation.
- We do not claim any specific airport is vulnerable.
- We do not claim to know what capabilities the FAA may have deployed and not disclosed.
- We do not claim the novel *HAIJACKED* is a forecast.
- We claim that this layer is unauthenticated, that it has been publicly demonstrated, and that the current modernization program does not appear to address it.

Items reported but not yet independently verified for this document (and therefore excluded from operative claims): a DOT Office of Inspector General finding reported April 2026 regarding baseline security controls on a portion of high-impact ATC systems; a reported January 2021 arrest in Berlin for ATC impersonation. Both remain marked for verification.

7. Recommended Question for the Record

The purpose of this campaign is not a drafted bill and not a prescribed technical architecture. It is a single question, asked on the record, at any hearing touching FAA modernization or artificial intelligence in critical infrastructure:

“Does the air traffic control modernization program include any capability to verify that a voice transmitted on an ATC frequency belongs to an actual controller? If not, why not — and what would it cost to add?”

Notes and Sources

1. Vu & Wei (2026), § III — threat model stating the absence of cryptographic authentication and encryption on legacy VHF voice. ICAO Doc 4444 governs phraseology and ATM procedure; it is not a source for cryptographic claims.
2. Andrew Logan, “Voice Cloning Air Traffic Control: Vulnerabilities at Runway Crossings,” DEF CON 33 Main Track, August 10, 2025.
3. Aviation International News, “DEF CON Talk Warns of ATC Voice Cloning ‘Nightmare,’” August 22, 2025.
<https://www.ainonline.com/aviation-news/2025-08-22/def-con-talk-warns-atc-voice-cloning-nightmare>
4. Dao Vu & Peng Wei, “Generating Realistic Air Traffic Control Voice Communication using AI-based Text-to-Speech Models,” George Washington University; IEEE ICNS 2026, Herndon, VA, April 14–16, 2026 (peer-reviewed conference paper). Threat model § III; ATCOSIM evaluation § V-A; results § V-B, Table I; limitations § VI.
<https://bpb-us-w2.wpmucdn.com/web.seas.gwu.edu/dist/9/15/files/2026/04/Dao-DeepFakeATC-Comms-ICNS26.pdf>
5. Reconciliation bill (H.R.1) appropriations, signed July 4, 2025; program targets as publicly described for radar replacement and telecom migration. (Not the 2024 FAA Reauthorization Act.)
6. DEF CON 33 talk recording: <https://www.youtube.com/watch?v=JKwxsGYcZq4>
7. ABC News, “Hackers Attack Air Traffic Control,” August 29, 2000. <https://abcnews.go.com/US/story?id=95993>
8. SKYbrary, “Unauthorised Use of ATC Frequency.” <https://skybrary.aero/articles/unauthorised-use-atc-frequency>
9. FAA staffing data (controller deficit and May 15, 2026 target revision); NATCA for the figure that more than 41% of certified controllers work 10-hour days, six days per week.
10. Criminal statutes: 49 U.S.C. § 46308; 18 U.S.C. § 32 (incl. § 32(a)(8)); 47 U.S.C. § 333. Synthetic-media legislation cited for context only: TAKE IT DOWN Act (S.146); AI Fraud Accountability Act of 2026 (S.3982); NO FAKES Act of 2026 (S.4591).

Corrections invited. See <https://haijacked.com/humans.txt>. The authors have not built, tested, or transmitted any synthetic ATC audio and will not. There is no demonstration, audio, simulation, or tooling on haijacked.com.