US Ops Update: Privacy, IDs & Safety

Chris Shieff
31 March, 2025

Key Points

- **FAA Enhances Aircraft Privacy:** The FAA now allows private aircraft owners to request the removal of personal details from public FAA websites, enhancing privacy.
- **US Address Required Abroad:** FAA certificate holders abroad must nominate a physical US address by April 2 (for new applicants) or July 7 (for existing holders) to retain their privileges, with professional services available for those without a US address.
- **REAL ID Deadline Looms:** From May 7, all adult passengers on US commercial flights (including Part 135 charters) must present a REAL ID-compliant ID or other accepted identification, with private Part 91 flights exempt.
- **Notam System Fails Again:** The US Notam system suffered another outage on March 22, raising concerns about its reliability.
- **FAA Tightens KDCA Helicopter Rules:** After the Jan 29 mid-air collision, the FAA has closed a KDCA helicopter route, restricted non-essential ops, mandated ADS-B Out, and launched a broader safety review.
- **KDCA Drone Tests Trigger Alerts:** On March 1, military counter-drone testing near KDCA triggered erroneous TCAS alerts, raising concerns over improper testing and its impact on civil aviation.

In Cognito

On March 28, the FAA began accepting requests from private aircraft owners to **withhold personal details** (such as name and address) from public access across all FAA websites.

It’s good news for business aviation, as it potentially makes it more difficult for members of the public to track the movement of **privately owned aircraft** for nefarious purposes.

Aircraft owners can now submit their request via the Civil Aviation Registry (CARES) here.

Address for Service

Attention all **FAA License holders abroad** – this one's for you!

The FAA has written a new rule that will require certificate holders abroad to nominate a physical **US address for service**. We've written about it in detail here, but there are essentially two looming deadlines to be aware of:

April 2 for new applications, and **July 7** for anyone who already holds FAA certificates, ratings or authorizations. You'll need to submit this via the USAS website that is about to go live.

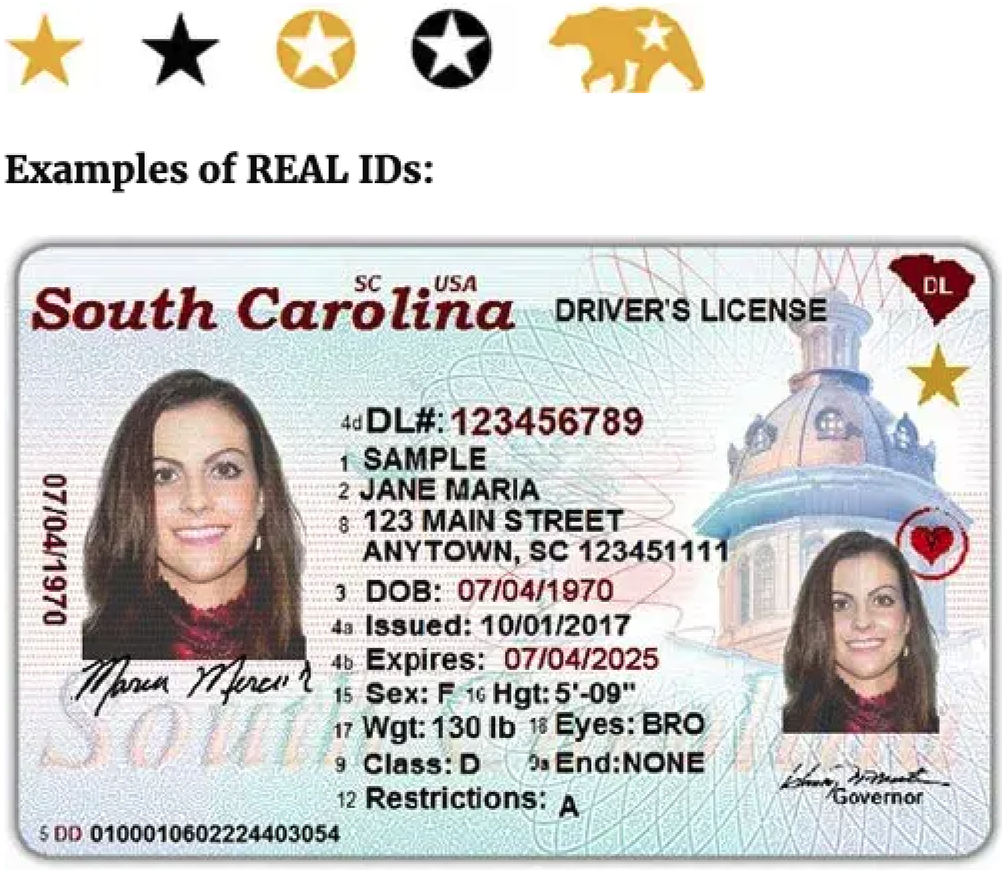
Whatever you do – don't ignore this. If you don't nominate a US based address by the applicable date, you won't be able to exercise the privileges of your document. i.e. say sayonara to your license until you submit the right info.

If you don't have an address to nominate in the US, don't despair. You can use a professional service like FAA Mail Agent. These guys can take care of all it for less than 50 bucks a year. Use the code 'Opsgroup' and get a discount.

Passenger ID Requirements

From May 7, all adult passengers (18+) using commercial air transport within the US (including Part 135 charters) **must show an ID** that complies with the new Real ID Act.

The big change is that anyone who wants to use a state-issued ID or drivers licence to meet this requirement must make sure that it is REAL ID compliant – look for one of the following symbols:



Examples of REAL IDs:

SC USA

South Carolina DRIVER'S LICENSE

DL

4d DL#: 123456789

1 SAMPLE

2 JANE MARIA

8 123 MAIN STREET
ANYTOWN, SC 123451111

3 DOB: 07/04/1970

4a Issued: 10/01/2017

4b Expires: 07/04/2025

15 Sex: F 16 Hgt: 5'-09"

17 Wgt: 130 lb 18 Eyes: BRO

9 Class: D 9a End:NONE

12 Restrictions: A

07/04/1970

Governor

5 DD 0100010602224403054

There is also a list of other IDs (such as US and Foreign Passports) that continue to be acceptable.

Operators need to take note because if they allow a passenger to board an aircraft without the appropriate ID they are effectively breaching TSA requirements and become liable for hefty penalties

Important note – private flights operated under **Part 91 are exempt.**

The Notam system went kaput (again).

The US Notam system was down (again) for several hours on March 22 due to a hardware failure. It was the second time since early February.

The cause of the latest outage was a hardware failure.

Once again we **collectively flinched** – a system crash in January 2023 lead to the first US ground stop since 2001, disrupting over 10,000 flights.

Questions are being asked about the reliability of the system, and its lack of redundancy.

The FAA previously announced plans to discontinue the legacy US Notam system by mid-2025, with further changes slated for the next five years.

There appears now renewed public and political concern for a **faster resolution.**

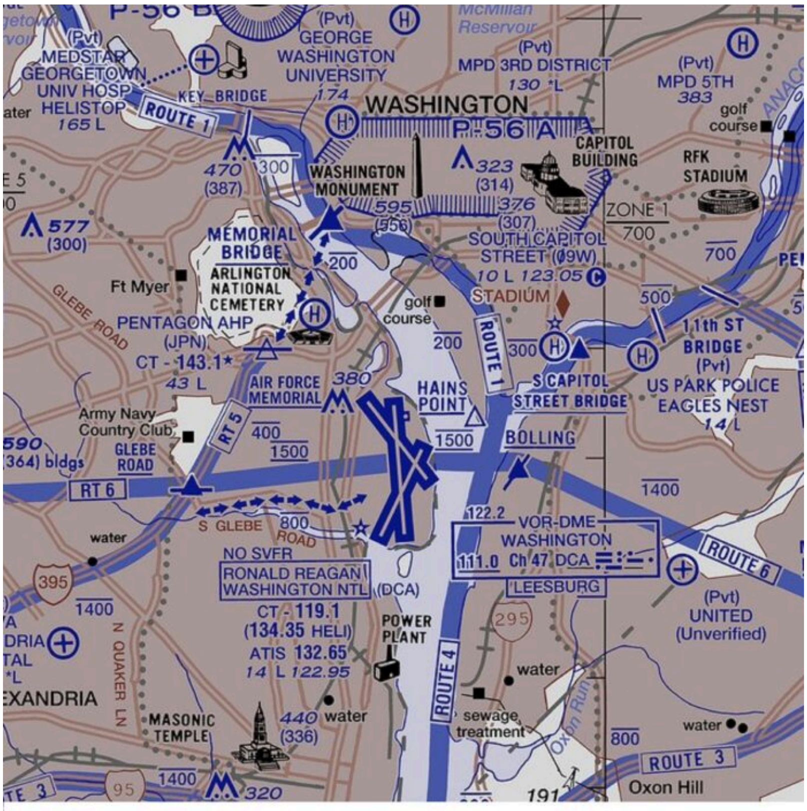
Mixed Traffic and The Potomac Tragedy

The FAA has responded to several recommendations made by the NTSB in its preliminary report from the mid-air collision over the Potomac River on January 29.

The immediate changes will be felt at **KDCA/Washington itself.** The FAA has permanently closed the low level helicopter route involved in the accident. Non-essential helicopter ops will also be banned, with increased ATC separation applied to those on ‘urgent missions.’

ADS-B out is now mandated for all helicopters, with only very limited exemptions for presidential missions.

Further afield, the FAA is also looking closely into ops at airports in other major cities with high volumes of **mixed traffic** (including NY, Boston, Chicago, Dallas, Houston and LA) with corrective actions looming for any risks identified.



RT 1: AMERICAN LEGION BRIDGE OVER POTOMAC RIVER, EAST OF ROOSEVELT ISLAND TO THE TIDAL BASIN. OVER WASHINGTON CHANNEL TO ANACOSTIA RIVER. NORTHEAST OVER ANACOSTIA RIVER TO RIVERDALE AND VIA BALTIMORE WASHINGTON PARKWAY TO GREENBELT.

ALTITUDES: AMERICAN LEGION BRIDGE AT OR BELOW 1300 FEET MSL, CHAIN BRIDGE AT OR BELOW 700 FEET MSL, KEY BRIDGE AT OR BELOW 300 FEET MSL, MEMORIAL BRIDGE AT OR BELOW 200 FEET MSL NOT ABOVE 200 FEET MSL UNTIL JAMES CREEK MARINA, AT OR BELOW 300 FEET MSL TO 11TH STREET BRIDGE, AT OR BELOW 500 FEET MSL TO PENNSYLVANIA AVENUE, AT OR BELOW 700 FEET MSL FROM PENNSYLVANIA AVENUE TO RIVERDALE, AT OR BELOW 1300 FEET MSL TO GREENBELT. (HELICOPTERS CROSSING POTOMAC RIVER TO OR FROM THE PENTAGON SHALL BE AT OR BELOW 200 FEET MSL).

RT. 4: FORT WASHINGTON OVER POTOMAC RIVER TO WILSON BRIDGE. THEN VIA EAST BANK OF POTOMAC RIVER TO ANACOSTIA RIVER. INTERCEPT ROUTE 1 AT ANACOSTIA RIVER.

ALTITUDES: AT OR BELOW 1000 FEET MSL AT FORT WASHINGTON, DESCEND TO 600 FEET MSL ABEAM BROAD CREEK INLET, BEGIN DESCENT FROM 600 FEET MSL TO ARRIVE AT 300 FEET MSL OVER WILSON BRIDGE, THEN AT OR BELOW 200 FEET MSL NORTH OF WILSON BRIDGE.

The FAA has announced it will permanently shutter the low level helicopter Route 4.

TCAS wasn't spoofed in Washington.

On March 1, several aircraft on approach to **KDCA/Washington** responded to **erroneous TCAS alerts**, including RAs. While recent research has indicated malicious interference of TCAS is a credible security concern, a Senate hearing last week revealed this was not the case.

The culprit was counter-drone testing by the military nearby which was operating on a similar spectrum to TCAS – a separate concern previously raised by the FAA.

Nevertheless, there are concerns that these tests were **conducted improperly** and caused unnecessary alarm to civil aircraft nearby. At the very least it was an unfortunate coincidence given recent events at the airport.

Other things you might have missed.

- *TFR Busts* – The FAA has reported several instances of civil aircraft busting TFRs in recent weeks. The hot spot appears to be **Palm Beach, FL** where the President has a residence at

Mar-a-Lago nearby. A reminder that special procedures apply, including TSA Gateway screening when active for anyone headed in or out of **KPBI/Palm Beach.** More on that in our recent article, here.

- *Laser Strikes* – New guidance was published by the FAA on March 26. Turns out the number of laser strikes on aircraft continue to be **dangerously high.** There's an online tool to see where the worst spots are here. Remember to report em!
- *Drones* – DJI, the main recreational drone producer in the US, has removed its built-in geo-fencing feature that physically protects airports from incursions. Instead, an FAA database will simply warn the user when close to a no-fly zone. The issue is that this can now be **maliciously ignored.** DJI has said that its geo-fencing is about education, not enforcement. We're not convinced – continue to report any illegal sightings to the FAA.

Anything we missed?

Let us know via news@ops.group, and we'll add it to this article. As always the team is also available to help answer any questions, or put you in touch with the person who can.

DC False Alerts: Could TCAS Be Vulnerable to Cyber Attack?

Chris Shieff
31 March, 2025

On March 1, several aircraft reported erroneous TCAS TA and RA alerts while on approach to Runway 19 at **KDCA/Washington.** All aircraft correctly followed avoidance procedures, and **no loss of separation** occurred. Six of the incidents occurred within eleven minutes of each other.

⬆ *shared with permission, courtesy of **VASAviation.***

What has followed is speculation – who, or what, was responsible? It is an answer the FAA is actively seeking.

TCAS interference is rare but can occur. There are several plausible explanations including ground clutter and reflections, software issues and unintentional radio interference.

However, it would be hard to deny that these alerts came at a **sensitive time** both for operations at the airport following the mid-air collision over the Potomac River, and across a broader tapestry of concern for aviation safety across the US NAS given recent events.

Which begs an important question – **can TCAS actually be tampered with?** Is it possible these events were an act of criminal mischief or other mis-intent? While remote, a little-known alert issued just weeks ago by **CISA** (the part of Homeland Security responsible for US cyber and infrastructure security) suggests it is *indeed* possible.

Published on January 21, CISA discussed **two flaws in TCAS design** that leave the system vulnerable to **malicious cyber-attacks** – one of which they deem a high, almost critical vulnerability.

In event that such an attack occurs, criminal interference could generate fake targets on an aircraft's TCAS display and even disable resolution advisories.

The problem is that bulletin is quite technical. So here is a break-down of what it says in plain, simple language.

The Bulletin

There were essentially two risks identified for TCAS II Versions 7.1 or older.

1. Fake Position Signals

It is theoretically possible to broadcast a spoofed aircraft location to another target.

This could be achieved using specialised radio equipment where potential attackers could send fake signals to aircraft, causing the appearance of **non-existent targets** on TCAS displays, along with the associated warnings.

In other words, crews would effectively be chasing shadows.

As TCAS II systems rely on transponders that may not be able to adequately validate the data received, they remain vulnerable to unauthorised signals. The bulletin describes this risk as a reliance on '*untrusted inputs'.*

Read the report and you'll see something called a '**CVSS score.'**

CVSS stands for **Common Vulnerability Scoring System**, and it is basically a danger rating for flaws in computer security. It is a measure of how serious a vulnerability is. Factors include the method of attack, the access required and the potential impact.

It is represented on a scale of 0 (non-existent) to 10 (critical).

The issue of fake position signals has been given a CVSS score of 6.1.

Perhaps more concerning is that the report advises there is no way to actively mitigate this threat with existing TCAS technology. The equipment required is accessible to the public. Therefore this threat is the most likely suspect of any erroneous TCAS interference occurring today.

2. No TCAS RA

This affects some older TCAS II systems using transponders with outdated technical standards.

It is theoretically possible for an attacker to impersonate a ground station and send a special request that lowers a system's sensitivity settings. A TCAS sensitivity level command does exist, envisaged to reduce nuisance alerts at some airports.

This could be used to maliciously adjust sensitivities to the lowest setting and even **disable a resolution advisory** completely.

The threat has a concerning CVSS score of 8.1 – highly vulnerable to exploitation, but would require a high level of expertise and technology to carry out.

Fortunately, in this case there is a way to mitigate the problem – by switching to ACAS X, or upgrading your associated transponder to more recent technical standards.

There is **no indication** that this has vulnerability has ever been exploited.

So, could the aircraft at KDCA have been hacked?

It's unlikely, but CISA's report indicates it's possible. And a new expert analysis of events at KDCA by **Aireon** seems to agree. In their published report they found that *'it is possible the intruder was airborne or related to a ground-based transmitter used for testing or spoofing.'*

Why does this matter?

The industry must remain responsive to security threats that are becoming increasingly sophisticated and designed to exploit vulnerabilities in safety critical systems.

The recent industry-wide interest in GPS interference spanning from the inconvenient, to major degradations including the loss of EGPWS protection, ADS-B tracking and navigational accuracy is a startling testament to this fact. This is all possible because of **existing system design.**

Since the events of September 11, passenger screening and security protocols have undergone a revolution, and it's now much harder for bad actors to carry out conventional attacks. But there are still risks associated with malicious attacks that could potentially be achieved **remotely** – and cyber-interference seems an obvious choice.