

UAP and Aviation Safety: Detection, Notification Duties, and Government Liability

Version 1.10 · October 2026 · nhilaw.com/issues/d4.html

Version 1.10, October 2026. Legal information, not legal advice. Published by the [Emergent Frontiers Institute](#) (NHI Law is not a law firm). Citations checked in October 2026; check every citation before relying on it.

Key points

- No statute requires the military or intelligence community to share classified UAP detections with the FAA or pilots; the reporting rules (FAA notices, the 2023 Joint Staff order) send information inward to AARO.
 - FTCA claims face the discretionary function exception (*Allen*; *Varig*); claims built on violation of a mandatory directive or on operational negligence survive.
 - Pilots who are disciplined for reporting have an AIR21 remedy now (49 U.S.C. §42121; 90 days).
 - After any incident, send preservation demands to the FAA, NORAD, the units involved and AARO, and ask the NTSB to obtain military data ([Form D4-1](#)).
 - The fix is legislative: a duty to share safety-relevant detections with the FAA in usable form and a compensation scheme.
-

1. Summary

Military and intelligence sensors detect objects in or near civil airspace that civil air traffic control cannot see or cannot identify. If a UAP causes or contributes to a civil aviation accident or near miss, victims will ask whether the government knew of the hazard and failed to warn.

The law gives limited support for that claim:

- **No general statutory duty** requires the Department of War or the intelligence community to share classified sensor detections with the FAA or pilots. The FAA's own procedures since October 2025 require controllers to report UAP observations upward (FAA Notices N7110.800 and N7210.970), and Congress has directed AARO to report UAP intercepts by NORAD and NORTHCOM to Congress (50 U.S.C. §3373(1)(5)). The pending Safe Airspace for Americans Act would route pilot reports to AARO and protect reporting pilots.
- **FTCA claims** face the discretionary function exception, 28 U.S.C. §2680(a). Decisions about whether and how to warn the public of hazards known through classified programs have

been held discretionary. *Allen v. United States*, 816 F.2d 1417 (10th Cir. 1987) (fallout from atomic tests; the Atomic Energy Commission's monitoring and warning programs were protected policy judgments). Once the government undertakes to provide a service, such as air traffic control, it must perform it with due care. *Indian Towing Co. v. United States*, 350 U.S. 61 (1955); *Ingham v. Eastern Air Lines, Inc.*, 373 F.2d 227 (2d Cir. 1967) (FAA approach controller's failure to tell an incoming aircraft that visibility had dropped, in violation of an FAA directive requiring transmission of weather changes, was negligence).

- **Military operations** face additional defenses: the combatant activities exception (§2680(j)), *Feres* for service members, and the state secrets privilege.
- **Statutory compensation** has been Congress's answer when courts denied relief for secret government hazards (Radiation Exposure Compensation Act, 1990, after *Allen*).

The practical recommendation is legislative: a statutory duty to share safety-relevant UAP detections with the FAA in usable form, a confidential pilot reporting channel, and a compensation scheme for injuries traceable to UAP or to government operations against them.

2. Current reporting framework

- **FAA Notice N7110.800** (Sept. 12, 2025) amends JO 7110.65 (Air Traffic Control) to require controllers to inform the supervisor or controller-in-charge of reported or observed UAP activity. **FAA Notice N7210.970** (Sept. 25, 2025) amends JO 7210.3 to require notification to the national security and operations office (NTSO ATSC) and to provide the AARO reporting link. Both were effective October 26, 2025, with cancellation dates of January 22, 2026. The controller requirement is now permanent: JO 7110.65BB Change 2 (effective January 22, 2026) cancelled and incorporated N7110.800, retitled Chapter 9, Section 8 "Unidentified Anomalous Phenomena (UAP) Reports," and provides in §9-8-1 that controllers "[i]nform the operations supervisor/CIC of any reported or observed unidentified anomalous phenomena (UAP)/unexplained phenomena activity," with a cross-reference to JO 7210.3 §4-7-4. The Pilot/Controller Glossary now defines UAP for aviation reporting purposes and refers to AARO for the full definition. The facility-level rule is also permanent: JO 7210.3EE §4-7-4 (Change 3, effective July 9, 2026) provides that "[p]ilot reports and/or air traffic personnel observations of unidentified anomalous phenomena (UAP) activity must be reported to the National Tactical Security Operations (NTSO) Air Traffic Security Coordinator (ATSC) team on the Domestic Events Network (DEN)," with the reporting aircraft's call sign and position, the UAP's position and description, and whether it appeared on ATC radar. Both rules send information up to security coordinators; neither requires controllers to broadcast a UAP hazard to other aircraft, which remains a matter for the controller's general duty to issue safety alerts and traffic advisories.
- **Military reporting runs inward.** The Joint Staff J3 GENADMIN, "Unidentified Anomalous Phenomena Reporting and Material Disposition," DTG 191452Z May 2023, released under FOIA as DoD 24-F-0067, requires combatant commands and services to report every UAP "incident," "incursion," and "engagement" to AARO (incident and incursion reports within 96 hours, engagement reports within 12 hours, §§3.C.1-3.C.2), to notify counterintelligence

within 24 hours, and to transfer raw data and recovered material to AARO-designated locations within 30 days (§§3.E-3.F). Commands must also receive reports “from third parties-to include civil and foreign partners” (§3.G.1.A.1). Nothing in the order requires any notice back to the FAA, air traffic control, or civil operators, and reports are classified under the UAP Security Classification Guide (§4.D). The order therefore documents a one-way flow: civil reports go into the military system, and military detections are not routed to civil aviation. That gap is the factual premise of a failure-to-warn claim and supports a request for a notification rule ([Form D4-1](#)).

- **AIM 7-7-4** (Aeronautical Information Manual, Change 3, effective July 9, 2026), titled “Unidentified Anomalous Phenomena (UAP) Reports,” tells pilots who want to report UAP activity to “visit the All-Domain Anomaly Resolution Office (AARO) website” and, “[i]f concern is expressed that life or property might be endangered,” to report it “to the local law enforcement department.” The paragraph says nothing about reporting a UAP hazard to air traffic control so that other aircraft can be warned; a controller who does receive a report must inform the operations supervisor under JO 7110.65BB §9-8-1.
- **50 U.S.C. §3373(1)(5)** (FY2026 NDAA §1671): AARO briefings on NORAD and NORTHCOM intercepts.
- **NASA ASRS**: the NASA UAP Independent Study Team recommended adapting the Aviation Safety Reporting System for confidential UAP reports.
- **Safe Airspace for Americans Act**. Introduced as H.R. 6967 (118th Cong., Jan. 11, 2024) and again as H.R. 5231 (119th Cong., Sept. 9, 2025; Reps. Garcia, Grothman, Moskowitz, Ogles), referred to Transportation and Infrastructure and to Oversight; as of October 2026 the bill had no recorded action beyond added cosponsors. H.R. 5231 would require the FAA, within 180 days, to set procedures for collecting and investigating UAP incidents reported by aircrew, controllers, and other aviation personnel, including “immediately archiving” pilot-controller communications and radar data (§2(a)(4)); share all reports and data with AARO (§2(c)); bar use of reports in enforcement except for accidents or crimes (§2(d)); bar consideration of UAP reports in airman medical and competency certification (§2(g)-(h)); and prohibit reprisal by federal agencies, contractors, and air carriers, including cease-and-desist letters (§2(i)-(j)). Like the Joint Staff order discussed above, the bill moves information from civil aviation to AARO; it contains no requirement that DoD or AARO warn the FAA or operators of hazards detected by military sensors.

2.1 Pilots who report

A pilot who reports a UAP and is disciplined or grounded by an airline for it has a federal remedy. AIR21, 49 U.S.C. §42121, forbids an air carrier, a contractor, or a subcontractor to discharge or discriminate against an employee who provides information about a violation, or alleged violation, of an FAA order, regulation, or standard, or any federal law relating to air carrier safety; the employee must file with the Secretary of Labor within 90 days. A report under the FAA’s own UAP procedures, or a report of a hazard to safety of flight, fits the statute. The pending Safe Airspace for Americans Act would add UAP-specific protections (below), but AIR21 applies now. [Issue D7](#) covers pilots’ remedies, FAA investigations, and medical certification in full ([Form D7-1](#)).

2.2 Airspace closures

The FAA restricts airspace through temporary flight restrictions issued by NOTAM, including around hazard areas (14 C.F.R. §91.137), and through special security instructions issued “pursuant to agreement between the FAA and the Department of Defense, or between the FAA and a U.S. Federal security or intelligence agency” (§99.7). The February 2023 shootdowns were preceded by closures of this kind. Records of who requested a restriction, and why, are the first records to request after any incident ([Form D4-1](#)).

2.3 What the military sees and civil controllers do not

A former director of the Navy’s UAP Task Force writes that FAA air traffic control is “blind to anything without a transponder,” so an object detected by military sensors near an airliner may never reach the controller (Jay Stratton, *Out of the Shadows* ch. 44 (2026)); the same author describes a near midair collision between Navy aircraft and an unidentified object on December 13, 2014 (*id.* ch. 24). On the site’s premise, the gap is deliberate as well as technical: the military reporting chain runs to AARO, an office the site assumes is part of the concealment, and nothing requires AARO or the commands to pass hazard information back to the FAA.

3. FTCA analysis

3.1 Discretionary function

The exception bars claims “based upon the exercise or performance or the failure to exercise or perform a discretionary function or duty,” 28 U.S.C. §2680(a). Under *Berkovitz v. United States*, 486 U.S. 531 (1988), and *United States v. Gaubert*, 499 U.S. 315 (1991), conduct is protected if it involves judgment or choice not controlled by a mandatory directive and is susceptible to policy analysis.

- **Decisions about whether to disclose classified detections** to the FAA or the public involve security trade-offs and will usually be protected. *Allen* is the closest precedent: the government’s choices about monitoring and informing the public of fallout risks were protected even though the plaintiffs suffered grave harm.
- **FAA oversight decisions** are a hard case for plaintiffs. The Supreme Court held that the FAA’s decision to “spot-check” aircraft for compliance with safety standards was a discretionary policy choice. *United States v. S.A. Empresa de Viacao Aerea Rio Grandense (Varig Airlines)*, 467 U.S. 797, 819-20 (1984). A claim that the FAA should have built a system to detect or share UAP information meets *Varig*; a claim that a controller failed to follow an existing UAP reporting rule does not.
- **Mandatory directives** defeat the exception. If a regulation, order, or statute requires a specific notification (for example, the FAA notices for controllers, or a DoD instruction requiring notice to the FAA of hazards to aviation), a failure to follow it is not protected. Practitioners should obtain all applicable orders (FAA JO 7110.65, JO 7610.4 (special operations), NORAD and DoD airspace coordination instructions).
- **Operational negligence** in performing a service already undertaken (for example, a controller who receives a UAP hazard report and fails to relay it) is generally not protected.

3.2 Other FTCA limits

- **Combatant activities** (§2680(j)) bars claims “arising out of the combatant activities of the military or naval forces ... during time of war.” Its application to domestic intercepts is doubtful.
- **Feres v. United States**, 340 U.S. 135 (1950), bars service members’ claims incident to service.
- **State secrets** ([Issue A1](#)) may block proof of what the government knew.
- **Foreign country exception** (§2680(k)) for injuries abroad.

3.3 Contractor liability

Contractors operating sensors or conducting tests may be sued under state law. After *Hencely v. Fluor Corp.*, 608 U.S. 31 (2026), preemption is unlikely where the contractor’s conduct was not required or authorized by the government. The government contractor defense (*Boyle v. United Technologies Corp.*, 487 U.S. 500 (1988)) applies to design defects in military equipment that conform to government specifications.

4. International aviation law

The Chicago Convention (1944) and its Annexes (Annex 11 air traffic services; Annex 13 accident investigation) require states to provide air traffic services and investigate accidents. Under Annex 13, Chapter 5, the State of Occurrence institutes and conducts the investigation, and other States are expected to provide, on request, the information they hold that is relevant to it. If a UAP were implicated in an accident abroad, the foreign investigating authority could ask the United States for military radar and sensor data; the United States would answer subject to its national security limits, and Annex 13’s standards are obligations of states, not rights a private party can enforce in U.S. court.

4A. Accident investigation

The NTSB investigates “each accident involving civil aircraft” and, “with the participation of appropriate military authorities, each accident involving both military and civil aircraft” (49 U.S.C. §1132(a)(1)). An NTSB investigation has priority over any other federal agency’s investigation, except where the Attorney General suspects a criminal act (49 C.F.R. §831.5(a)(1)). Counsel for victims should ask the NTSB at the outset to request military radar and sensor data, since the Board’s priority is the strongest lever a private party has to get that data into the record.

5. Practice points

1. After any incident with a possible UAP factor, send preservation demands to the FAA, NORAD/NORTHCOM, the relevant military units, and AARO ([Form A3-2](#) adapted; [Form D4-1](#)).
2. Request NTSB involvement and data from all sources, including military radar.
3. Identify mandatory directives that required notification.

4. File FTCA administrative claims (SF-95) within two years (28 U.S.C. §2401(b)).
5. Consider contractor defendants in state court.
6. For a pilot client disciplined after a report, file an AIR21 complaint with OSHA within 90 days.
7. For passengers on international flights, the carrier's liability is governed by the Montreal Convention (Issue E5).
8. Advocate for statutory compensation if discretionary-function barriers block recovery.