WHITE PAPER · Infrastructure Dependency Risk

The November 13, 2026 nationwide ground stop: competing explanations

Nationwide ground stop, November 13, 2026

Carl Southwell, PublicRisk.ai

November 21, 2026

Status of this analysis

ILLUSTRATIVE. Built only from public reporting, not FAA network topology. Every hypothesis, including the official one, is a model of what could have happened; none is established. Structure assumed where the record is silent is tagged opinion.

12 explanations tested · 11 fit the facts · official account unaudited

In plain terms

This part is written for readers without a technical background. The numbered sections that follow give the full analysis, sources and method.

What happened

On the afternoon of Friday, November 13, 2026, the Federal Aviation Administration (FAA) stopped every departing flight in the United States for more than four hours. Controllers at 17 of the 22 regional centers that guide planes between airports began losing parts of their radio and radar picture. Every plane already in the air landed safely, but about 12,000 flights were canceled that day (not all because of the stop) and disruption lasted into the weekend.[1]

The FAA's explanation is that a new network device, being installed that day at a remote radio site in Arkansas by the company that runs the FAA's private communications network, flooded that network with connection requests, and older equipment on it could not cope. During the stop, the contractor took several hours to work out where the flood was coming from, which delayed getting flights moving again. Three days earlier the FAA had also switched on a new artificial-intelligence traffic tool at every regional center. The FAA says the two are unrelated.

No one independent of the FAA and its contractor has yet checked the official account. This paper sets out the realistic alternatives, shows which ones fit the facts, and says what evidence would settle the question and what should change regardless of the answer.

What might have caused it

We tested each possible explanation against what was observed: would that failure, spreading through the network's known dependencies, knock out as many control centers as actually went down?

[1] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers; Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop; CBS News: During nationwide ground stop, L3Harris struggled to find location of system outage (2026-11-18). https://www.cbsnews.com/news/ground-stop-l3harris-system-outage/. Accessed 2026-11-18.

Table 1. Estimate: current expert judgement of how likely each explanation is (see Expert valuation).

	Possible explanation	On purpose?	Fits the facts?	Estimate
H1	A single new router installed in Arkansas misbehaved and flooded the network, and older equipment could not cope. **(the official account)**	No	**Fits the facts**	22%
H2	The fault lies in the model or settings shared by all the new routers; Arkansas just happened to be first.	No	**Fits the facts**	26%
H3	Nothing was wrong with the new router. The old equipment cannot handle ordinary modern traffic, so any upgrade could have set it off.	No	**Fits the facts**	15%
H4	The new AI traffic tool, switched on everywhere three days earlier, was already adding traffic to the same network, and the router flood pushed it over the edge.	No	**Fits the facts**	4%
H5	Traffic from the AI tool alone overloaded the network.	No	**Fits the facts**	1%
H6	Someone working on the installation set the new router up to fail on purpose, for money, a grudge or on someone else's behalf.	Yes	**Fits the facts**	1%
H7	A check, not a real candidate: if the AI tool had simply crashed on its own, only its own advice would have been lost, not the nationwide picture.	No	Does not fit	—
H8	A foreign intelligence service that had quietly broken into the network set the routers off, either on purpose or because its hidden tools malfunctioned.	Yes	**Fits the facts**	3%
H9	The new routers were tampered with before they arrived, so a hidden fault was installed everywhere they went and went off later.	Yes	**Fits the facts**	2%
H10	Someone, or a runaway AI program, got into the network through the connections the new AI traffic tool opened to every center three days earlier.	Yes	**Fits the facts**	1%
H11	A computer virus spread from router to router and made them flood the network.	Yes	**Fits the facts**	1%
H12	The outage was one piece of a coordinated attack that also hit Microsoft, a major bank and the NSA in the same week, each disguised as a routine glitch.	Yes	**Fits the facts**	1%
	A cause nobody has named yet	Unknown	—	23%

Eleven of the twelve explanations fit the facts equally well. The outage itself cannot tell us which one is right; only records the operator holds (device logs, network traffic, change tickets) can.

> **Has the official account been checked?**
>
> Not yet. As of November 17, 2026 the account comes from the FAA and the Secretaries of Transportation and Homeland Security. The FAA and L3Harris, the operator of the network, are investigating their own system. No independent root-cause report (NTSB, DOT Inspector General, GAO) has been published. The FAA Administrator said the router finding is not a full explanation of the root cause.[2]

Could someone have done this on purpose?

Six of the explanations involve someone acting on purpose (a foreign state, an insider, an outside party, criminals). All of them fit the outage as well as the accidental ones do, because the network fails the same way whatever sets it off. So the outage alone cannot rule them in or out.

The public record holds five pieces of evidence that fit a deliberate cause and no published forensic finding either way. Officials say they have seen no sign of an attack, but those are statements by the people investigating their own systems, and they have not ruled one out. Background facts make some of these explanations plausible without being evidence about this event, for example official warnings that foreign hackers have hidden inside U.S. transport networks.

What would rule it out: Routers still in their boxes match signed images, and the configuration template's history is clean. A sweep of the fleet against vendor images finds no unexplained code. Each operator's root-cause report traces its outage to a specific internal change with a timestamp and author, and no indicators are shared.

Our current estimate is that the chance it was deliberate is about 9%, against about 68% that it was an accident and 23% for a cause nobody has named yet. These are judgements on today's evidence and will move as records are published.

Was this part of something bigger?

Six other major outages happened close to this one, from one day before to four days after: Microsoft, the National Weather Service, JPMorgan Chase, Apple, the NSA's classified network and United Airlines. In four of them the only explanation so far comes from the organization that failed; outside confirmation exists for one. Most were blamed on a software update or other change, as the FAA's was.

There are three ways to read a cluster like this: Coincidence: Large systems fail often enough that several failing in one week can happen by chance. Related, not coordinated: a common driver: Nobody planned it, but the same pressure, such as rushing patches and upgrades out at the same time, made many systems fragile at once. Coordinated attack (explanation H12): Someone attacked several organizations on purpose and made each failure look like a routine glitch.

[2] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers; Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.

Remote possibilities are discussed rather than ranked. Even if the FAA failure is unrelated to the others, a common driver would mean the fix has to be made across sectors, not only at the FAA; and a coordinated attack, however unlikely, has consequences that justify checking it with evidence rather than statements.

Could the new AI tool have overloaded the routers?

Possibly, but probably not on its own. When engineers cut off the two field sites, the network settled down, and no one has reported switching the AI tool off. If it kept running, as seems likely, that points away from the AI tool as the sole cause, although the account of the recovery comes only from the FAA.[3]

The FAA's denial says the tool does not send information into air traffic control. It does not say how much traffic the tool creates while collecting data from every center. So it remains possible that switching the tool on everywhere, three days earlier, left the network with less spare capacity, and the router flood then pushed it over. Two sets of records would settle this: the network's traffic from November 10 to 13, and where the flood of connection requests came from. Neither has been published.

A separate question is whether someone, or a runaway AI program, could have used the tool's new connections to break in. That is explanation H10, covered under 'Could someone have done this on purpose?'

Would Starlink have helped?

Probably not in the way the public argument suggests. What failed on November 13 was not a broken connection. Equipment inside the FAA's network was flooded with traffic from the network itself. Adding a satellite link does not stop a flood: if the new link is plugged into the same network, the flood travels over it too.[4]

Where Starlink could help is as a separate, walled-off backup for the control centers' radio and radar connections, one the main network cannot reach. Our test shows a walled-off backup would have kept the centers connected under every explanation that fits the facts, and a backup joined to the main network would not have helped under any. A second ground network kept separate does exactly as well, so the benefit comes from the separation, not from satellites.

There are limits. The FAA's administrator has said Starlink would not be the only communications link for safety-critical services, and the transportation secretary says an earlier version had problems in FAA testing. Starlink suffered its own worldwide outage in 2025, and the FAA regulates SpaceX, which raises conflict-of-interest questions. Swapping one privately owned network the FAA cannot easily leave for another would repeat the problem the secretary now complains of.[5]

[3] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.
[4] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.
[5] Reuters via KFGO: US FAA not considering replacing L3Harris, Verizon contracts with Musk's Starlink (2025-07-16). https://kfgo.com/2025/07/16/us-faa-not-considering-replacing-l3harris-verizon-contracts-with-musks-starlink/; AOL: "Our airspace is very big": Sean Duffy defends FAA's decision to turn down free Starlink after Elon Musk's criticism (2026-11-18). https://www.aol.com/articles/airspace-very-big-sean-duffy-010848000.html; ThousandEyes: Starlink Outage Analysis: July 24, 2025. https://www.thousandeyes.com/blog/starlink-outage-analysis-july-24-2025; Bloomberg via Fortune: Elon Musk begins testing his Starlink terminals in the U.S. airspace system (2025-02-25). https://fortune.com/2025/02/25/elon-musk-begins-testing-his-starlink-terminals-in-the-u-s-airspace-system/; Reuters via Yahoo: US probes why a router installation sparked mass flight grounding (2026-11-16). https://www.yahoo.com/news/us/articles/us-probes-why-router-installation-182834297.html. Accessed 2026-11-18.

Should this have been handled as a cyberattack?

Possibly, and the federal rules allow for it, although they do not demand it for every outage. Civilian agencies must report security incidents to CISA, the government's cyber defense agency, within an hour of identifying them, including on systems run by contractors. 'Incident' has a legal meaning here: something that endangers a system without lawful authority, or that breaks the law or security rules. An honest mistake by an authorized contractor is not one, unless it broke those security rules. But the rules expect agencies to report before they know the cause: working out the cause is left until the end, and 'cause unknown' is an acceptable first report. At 3:30 p.m. on November 13 nobody knew the cause, so reporting it as a possible incident would have fit the rules. Whether it was required depended on whether the FAA thought an attack could not yet be ruled out. As of November 15, CISA had made no public statement about the event.[6]

There is a precedent for treating an accident this way. In 2024 a faulty CrowdStrike update crashed millions of computers. It was not an attack, yet CISA ran a coordinated response with the company and its partners, warned that attackers were exploiting the confusion, and tracked the root-cause report. Here, by contrast, the routers are being tested in the contractor's own lab, with FAA staff overseeing and the FBI invited, and as of November 15 CISA had said nothing in public. The federal board that used to review major cyber incidents has had no members since its members were dismissed in early 2025.[7]

Would CISA have had the people to do it? Since January 2025 the agency has lost almost a third of its staff, about 1,100 positions, in reductions led by DOGE and in budget cuts; those let go included members of its red teams, who simulate attacks to find weaknesses first. In June the homeland security secretary put CISA's staff at about 2,200 against a goal of 2,800. On November 18 he could not tell Congress how many work there now, while saying the agency 'has not missed a mission'. A smaller CISA has less capacity for exactly the work this kind of response needs: forensic checks, comparing evidence across that week's outages, and publishing what it found. Whether that was a limiting factor this time is not known, because CISA has said nothing in public about this event.[8]

Handling it as a possible attack does not mean accusing anyone, and it should never slow down getting planes flying again. It means copying the devices' memory and logs before they are reset, having someone outside the operator check them for tampering, comparing notes with the other organizations that failed that week, and publishing the conclusion. If it was an accident, that process proves it.

---

[6] CISA: Federal Incident Notification Guidelines (2017; revision pending as of November 2026). https://www.cisa.gov/federal-incident-notification-guidelines; 44 U.S. Code § 3552, Definitions (Legal Information Institute). https://www.law.cornell.edu/uscode/text/44/3552; BankInfoSecurity: Anatomy of the FAA Ground Stop: One Backbone, One Bad Change (2026-11-15). https://www.bankinfosecurity.com/anatomy-faa-ground-stop-one-backbone-one-bad-change-a-33396. Accessed 2026-11-18.

[7] CISA alert: Widespread IT Outage Due to CrowdStrike Update (2024-07-19, revised 2024-08-06). https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update; Reuters via Yahoo: US probes why a router installation sparked mass flight grounding (2026-11-16). https://www.yahoo.com/news/us/articles/us-probes-why-router-installation-182834297.html; BankInfoSecurity: Anatomy of the FAA Ground Stop: One Backbone, One Bad Change (2026-11-15). https://www.bankinfosecurity.com/anatomy-faa-ground-stop-one-backbone-one-bad-change-a-33396; ACM U.S. Technology Policy Committee: The Cyber Safety Review Board Should be Reinvigorated (2026-02). https://www.acm.org/public-policy/ustpc/policiesweb/csrb-2026; Fortune: Transportation secretary still doesn't totally rule out that a cyberattack may have hit the FAA, and the FBI is assisting the probe (2026-11-15). https://fortune.com/2026/11/15/cyberattack-hack-faa-air-traffic-control-communications-router-fbi-probe-sean-duffy-ground-stop/; Cybersecurity Dive: DHS disbands existing advisory board memberships, raising questions about CSRB (2025-01-22). https://www.cybersecuritydive.com/news/dhs-disbands-advisory-board-csrb/737976/. Accessed 2026-11-18.

[8] PolitiFact: Fact-checking DHS Secretary Mullin's hearing on FAA ground stop, outages, dirty bombs (2026-11-18). https://politifact.com/article/2026/nov/18/mullin-hearing-threats-outages-faa-delays/; USA Today via Yahoo: DHS Secretary Mullin won't say if cyber agency cuts were a mistake (2026-11-18). https://www.yahoo.com/news/politics/articles/dhs-secretary-mullin-wont-cyber-212852697.html; Broadband Breakfast: One Year After DOGE Cuts, Cybersecurity Agency Struggles Over Staffing (2026-06-13). https://broadbandbreakfast.com/one-year-after-doge-cuts-cybersecurity-agency-struggles-over-staffing/. Accessed 2026-11-18.

Did DOGE's cuts contribute?

It is possible but not shown. In February 2025 the FAA fired fewer than 400 of its 45,000 employees during the federal job cuts associated with DOGE, Elon Musk's cost-cutting effort. The transportation secretary said no air traffic controllers or critical safety staff were among them; the union for FAA technicians said hundreds of the people fired maintained air traffic control equipment. A congressman, as reported, blames the cuts for the outage, but that is a political claim, not a finding.[9]

The way cuts could have mattered is oversight of the contractor. The technicians' union says FAA staff normally assess the risk of a contractor's work and coordinate it, and that they were not involved this time. But the Washington Post, citing one person close to the investigation, reports that an FAA official supervised the Arkansas work and signed it off minutes before the outage. Government auditors have flagged weak contractor oversight at the FAA for four decades, long before DOGE.[10]

The cuts reached a second agency that matters here. CISA, which would lead any cyber investigation of the outage, lost almost a third of its staff in the same round of reductions (see 'Should this have been handled as a cyberattack?'). That cannot have caused the routers to flood the network, but it can limit how well the cause is investigated and how quickly any attack would be noticed.[11]

So DOGE is not a separate explanation of the failure; it is a possible reason why two safeguards, oversight of the contractor and the capacity to investigate, were weaker than they should have been. Three questions would settle the first: was an FAA risk assessment required for this work, was it done, and were the people who would have done it among those who left. For the second, the test is whether CISA attempted a forensic review and comparison with the other outages, and what stopped it if not.

What does the changing official story tell us?

The government's description of the cause has shifted. On November 14 officials blamed a newly installed router that flooded the network during a contractor's maintenance work. The next day he said he could not apologize for 'what was passed off to us', and on November 16 the president blamed 'very, very old equipment that had a heart attack' and said he took no responsibility. The head of the FAA has said the router finding is not the full explanation.[12]

At the same time, the White House tightened control of what officials say. On November 16 the homeland security secretary told Fox News that 'SI' (super intelligence, President Trump's preferred term for artificial intelligence) could be behind that week's outages. According to Politico, the new White House chief of staff,

[9] Reuters via Rappler: FAA fires fewer than 400 workers, transportation chief says (2025-02-18). https://www.rappler.com/world/us-canada/federal-aviation-administration-firings-february-17-2025/; CNN via Yahoo: Hundreds of FAA probationary workers fired by Trump administration, union says (2025-02-17). https://www.yahoo.com/news/hundreds-faa-probationary-workers-fired-041227806.html; WSHU: Himes blames Elon Musk, DOGE for nationwide ground stop (2026-11-16). https://www.wshu.org/connecticut-news/2026-11-16/faa-cuts-elon-musk-doge-nationwide-ground-stop. Accessed 2026-11-18.

[10] Aviation A2Z: FAA Union Says Nationwide Ground Stop Was Avoidable After Missing Risk Assessment (2026-11-16). https://aviationa2z.com/index.php/2026/11/16/faa-union-says-nationwide-ground-stop-was-avoidable-after-missing-risk-assessment/; MLQ.ai: FAA official supervised and signed off on the Arkansas repair work before the nationwide ground stop, Washington Post reports (2026-11-18). https://mlq.ai/news/faa-official-supervised-and-signed-off-on-the-arkansas-repair-work-before-the-nationwide-ground-stop-washington-post-reports/; GAO-26-107992: Air Traffic Control Systems: Ambitious New Modernization Effort Needs Cost and Schedule Planning (2026-09). https://files.gao.gov/reports/GAO-26-107992/index.html?pubDate=20260922. Accessed 2026-11-18.

[11] PolitiFact: Fact-checking DHS Secretary Mullin's hearing on FAA ground stop, outages, dirty bombs (2026-11-18). https://politifact.com/article/2026/nov/18/mullin-hearing-threats-outages-faa-delays/. Accessed 2026-11-18.

[12] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers; CBS News: A timeline of Trump administration's response to FAA ground stop (updated 2026-11-16). https://www.cbsnews.com/news/faa-ground-stop-trump-admin-response/; Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.

Stephen Miller, judged that off-script and took the secretary off television, handing public statements to the director of national intelligence and the secretary of state. A White House spokesperson then said there was no sign of 'malicious foreign cyberattacks or SI-related attacks'.[13]

None of this changes which explanations fit. 'A new router' and 'old equipment' are not rival facts: they are the two halves of a chain this paper already tests, the official account (the new router flooded the network) and the legacy-boundary explanation (the old equipment could not cope with ordinary modern traffic). Which half officials stress is a choice about where blame falls, not new evidence. Likewise, silencing one official's speculation neither proves nor disproves it, and a denial from the people who run the system is listed in this paper but not counted.

What it does show is that the official story is being settled by announcement while the FAA and L3Harris say they are still investigating the root cause. That is when an investigation by someone who does not run the system, publishing its evidence, matters most.[14]

What should change

These steps help whichever explanation turns out to be right:

- **Handle unexplained outages as possible cyber incidents from the first hour.** Until the cause is known, treat a big unexplained outage as a possible attack: report it to CISA as a possible incident, save the evidence, and keep restoring service at the same time.
- **Independent root-cause investigation.** Have someone who does not run the system find the real cause from preserved records, and publish the answer.
- **Inventory what the graph cannot see.** Map what the network depends on. Most of it is not on the public record, so other weak points may be hiding.
- **Protect the legacy boundary.** Put protective buffers wherever new equipment connects to old equipment, and set a firm date to retire the old equipment.
- **Split the shared layer into failure domains.** Divide the network into regions so a problem in one place cannot spread across the country.

These help if particular explanations are right:

- **Gate changes to the shared network.** Treat work on the shared network as risky: do it at quiet times, one site at a time, after testing, with a quick way to undo it. (if H1, H2, H4, H5, H6, H8, H9, H10, H11, H12)
- **Admission control at every site edge.** Make sure no single site can flood the whole network: cap how much each site can send and cut it off automatically if it misbehaves. The operator should also be able to see within minutes which site is causing the trouble. (if H1, H2, H4, H5, H6, H8, H9, H10, H11, H12)
- **Keep the owner's technicians in charge of contractor changes.** Before a contractor changes shared network equipment, the FAA's own technicians should assess the risk and sign off, and there should be enough of them to do it. (if H1, H2, H4, H5, H6, H8, H9, H10, H11, H12)

[13] The Independent via Yahoo: Stephen Miller puts Markwayne Mullin in 'primetime timeout' after bizarre TV appearance: report (2026-11-19). https://www.yahoo.com/news/politics/articles/stephen-miller-puts-markwayne-mullin-170152805.html; AlterNet: Top Trump official on TV 'timeout' after angering MAGA White House insiders (2026-11-19). https://www.alternet.org/trump-mullin-miller/. Accessed 2026-11-18.
[14] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers; Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.

- **Verify configuration integrity.** Keep tamper-proof records of how every device should be set up, and check the real devices against them. (if H6, H8, H9, H10, H11, H12)
- **Remove fleet-wide common mode.** Do not switch on a new feature on every device at once; try it at one site first. (if H2, H8, H9, H10, H11, H12)
- **Rule deliberate causes in or out with forensics.** Check the devices for signs of tampering with methods that would find it if it were there, and have someone outside the operator do it. (if H6, H8, H9, H10, H11, H12)
- **Close and watch third-party and AI connections.** List every outside company or system that can reach the network, including AI tools, cut what is not needed, and watch the rest. (if H4, H5, H8, H9, H10, H12)
- **Controls for AI and data-aggregation systems on shared networks.** Before an AI or data system goes nationwide, measure how much traffic it adds to shared networks and run it in a limited trial first. (if H4, H5, H10)
- **Correlate the week's outages.** Compare the technical evidence from that week's outages at different organizations to check whether anything links them. (if H8, H12)
- **Two-person rule for changes to shared network equipment.** Make sure no single person can change critical network equipment alone, and record every change. (if H6)

1 Technical summary

- 11 of 12 explanations reproduce the observed scope **(H3, H2, H1, H4, H9, H11, H12, H5, H10, H8, H6)**; H7 falls short.
- H3, H2, H1, H4, H9, H11, H12, H5, H10, H8, H6 lose the same service set; the graph cannot separate them (see 'What the evidence cannot yet separate').
- Official account **H1**: unaudited; rank 3 of 12 under the stated policy.
- H4 is a joint cause: each of its initial failures is necessary.
- Deliberate causes tested: H9, H11, H12, H10, H8, H6. Their counted support is limited to facts consistent with them; official denials and advisories are listed but not counted.
- Expert valuation (opinion): accidental 68%, deliberate 9%, not yet named 23%.
- No-regret measures: handle unexplained outages as possible cyber incidents from the first hour; independent root-cause investigation; inventory what the graph cannot see; protect the legacy boundary; split the shared layer into failure domains (see Recommendations).

2 The event

Instability at 17 of 22 Air Route Traffic Control Centers that spread into several TRACONs; some frequencies and radar feeds stayed up. Nationwide ground stop from about 15:30 ET to 20:15 ET; about 12,462 cancellations that day (not all caused by the stop).[15]

Scope used for the test: 17 of 22 centers. The graph models the 20 CONUS centers and is binary, so it marks a center lost where the record says unstable.

2.1 The official account and its audit status

L3Harris installed a new Juniper router at a remote radio site during the day. Its broadcasting function sent about 1,000 connection attempts every 4 to 5 seconds across FTI, and legacy TDM equipment serving the centers became unstable. Blocking the site restored stability. The FAA and L3Harris have since concluded that the Arkansas site caused the outage, though the contractor took several hours to locate it during the stop.[16]

Audit status: unaudited. As of November 17, 2026 the account comes from the FAA and the Secretaries of Transportation and Homeland Security. The FAA and L3Harris, the operator of the network, are investigating their own system. No independent root-cause report (NTSB, DOT Inspector General, GAO) has been published. The FAA Administrator said the router finding is not a full explanation of the root cause.

3 Method

Each explanation is a set of initial failures on the dependency graph plus any structure it has to assume that the public record does not show, such as a new system loading a shared network. The failure is propagated to a fixpoint (a node fails when every member of any one of its requirement groups has failed) and the services

[15] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers; Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.
[16] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers; Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.

lost are compared with the observed scope. For explanations with several initial failures, every proper subset is tested to establish whether each is necessary.

Claims. A claim counts when it is a statement of fact by an official or independent party. Denials by officials or interested parties are listed, not counted: a party denying its own fault is not evidence either way until audited. This page's own inferences are shown, never counted. Official facts count but stay unaudited. Context (an advisory, a precedent, an investigation status) makes an explanation plausible but is not evidence about this event: shown, not counted.

Ranking. Lexicographic, no weights: (1) reproduces the observed scope; (2) more counted supporting claims; (3) fewer assumed requirement groups; (4) fewer counted contradicting claims. A rank orders explanations for investigation; it is not a probability.

Completeness checks

- **Passed:** At least two alternatives to the official account are tested.
- **Passed:** A deliberate cause (insider, criminal, state actor) is tested, as it must be while the official account is unaudited.
- **Passed:** An accidental cause is tested.
- **Passed:** Every AI component in the graph is tested as a possible cause or path.
- **Passed:** A control case (an explanation expected to fall short) checks that the test can fail.

4 Competing explanations

Table 2. Explanations ranked by the stated policy. For / Against: counted claims. Denied: denials listed, not counted. Assumed: requirement groups an explanation adds to the graph.

#	Explanation	Initial failure (mode)	Lost	Observed scope	For	Against	Denied	Assumed
1	**H3 Legacy boundary** Alternative · accidental	Legacy TDM equipment carrying center radio and radar feeds (instability)	21	Reproduces 20/20	8	0	0	0
2	**H2 Fleet fault** Alternative · accidental	Broadcasting function on the new-router fleet (El Dorado, Amarillo, 60+ others) (connection_flood)	21	Reproduces 20/20	7	0	1	0
3	**H1 Official account** Official account · accidental	New router at El Dorado, AR radio site (installed by L3Harris, daytime) (connection_flood)	21	Reproduces 20/20	6	0	0	1
4	**H4 AI system coupling** Alternative · accidental	New router at El Dorado, AR radio site (installed by L3Harris, daytime) (connection_flood), SMART data collection from all centers (rollout and testing traffic, from 2026-11-10) (overload)	21	Reproduces 20/20	5	1	2	1
5	**H9 Supply-chain compromise** Alternative · deliberate (state)	Tampered firmware or standard configuration delivered with the new routers (tampered_firmware)	21	Reproduces 20/20	3	0	2	1
6	**H11 Self-spreading malware** Alternative · deliberate (criminal)	Self-spreading malware on the router fleet (malware)	21	Reproduces 20/20	3	1	2	1
7	**H12 Coordinated campaign** Alternative · deliberate (state)	Coordinated multi-sector campaign (FAA component) (intrusion)	21	Reproduces 20/20	3	1	5	1
8	**H5 AI system alone** Alternative · accidental	SMART data collection from all centers (rollout and testing traffic, from 2026-11-10) (overload)	21	Reproduces 20/20	3	2	2	1
9	**H10 Intrusion through the AI tool's data connections** Alternative · deliberate (unknown)	Unauthorized entry through SMART's new data connections (attacker or autonomous AI agent) (intrusion)	21	Reproduces 20/20	2	0	5	1

#	Explanation	Initial failure (mode)	Lost	Observed scope	For	Against	Denied	Assumed
10	**H8 Espionage or pre-positioned intrusion** Alternative · deliberate (state)	Unauthorized access to router management by a state actor (deliberate or a faulty implant) (intrusion)	21	Reproduces 20/20	2	1	5	1
11	**H6 Insider sabotage** Alternative · deliberate (insider)	Deliberate misconfiguration by someone with installation access (malicious_config)	21	Reproduces 20/20	1	1	1	2
12	**H7 Control** Control · accidental	SMART AI-supported traffic-flow system (expanded to all centers 2026-11-10) (outage)	1	Falls short 0/20	0	0	0	0

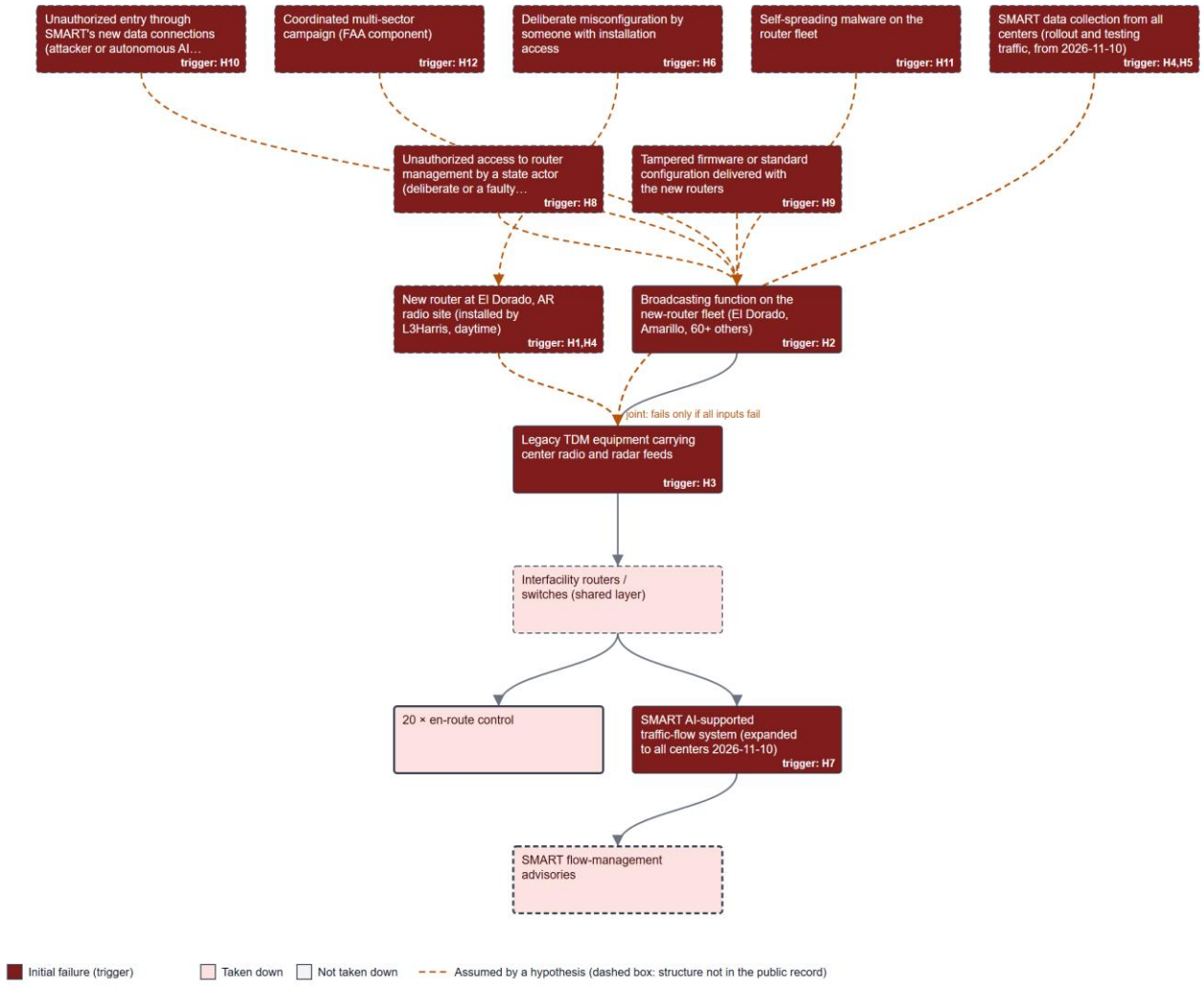


Figure 1. Dependency graph. Every node some explanation takes down; dark red marks the trigger, tint marks what is taken down, dashed lines and boxes mark structure an explanation assumes.

5 Evidence register

Every claim used in this paper, once, with who made it and what kind of statement it is. The explanations below refer to these numbers. Kind: fact (counted when from an official or independent party), denial (listed, not counted), context (makes an explanation plausible; not counted), inference (shown, not counted).

Table 3. Evidence register. Bears on: + supports, − contradicts.

#	Claim	Who, kind	Bears on
E1	Two potential locations: a radar site in Amarillo, Texas and a radio site in El Dorado, Arkansas, where L3Harris had deployed a new router. Blocking both stabilized the network.[17]	official (unaudited), fact	H1+, H2+, H5−
E2	The FAA disabled the same functionality on more than 60 other Juniper routers and paused installing them.[18]	official (unaudited), fact	H2+, H9+, H11+
E3	Asked whether modernization caused it: 'No, this is due to the legacy TDM system causing instabilities.'[19]	official (unaudited), fact	H3+
E4	The FAA says SMART is unrelated: it is a data aggregator and does not feed information into the air traffic control system.[20]	official (unaudited), denial	H4−, H5−, H10−
E5	The FAA has no indication of a cyberattack or an outside nefarious actor.[21]	official (unaudited), denial	H8−, H9−, H10−, H11−, H12−
E6	The router replacement was done in the middle of the day at a remote facility; the FAA will reevaluate when it does such work.[22]	official (unaudited), fact	H1+
E7	FAA Administrator Bryan Bedford said the router finding is not a full explanation of the root cause.[23]	official (unaudited), fact	H2+, H3+, H4+
E8	DHS Secretary Mullin said new FAA equipment and technology appeared to have overwhelmed older systems.[24]	official (unaudited), fact	H3+, H4+
E9	Mullin did not rule out the new AI tool when first addressing the press at the White House (a Latin Times headline quoted him: 'You Can't Rule Out Anything').[25]	official (unaudited), fact	H4+, H5+
E10	The FAA expanded SMART, an AI air traffic management system, to all centers on November 10, three days before the ground stop (The Washington Times).[26]	independent, fact	H4+, H5+, H10+

[17] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.
[18] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.
[19] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.
[20] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.
[21] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.
[22] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.
[23] Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.
[24] Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.
[25] Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.
[26] Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.

#	Claim	Who, kind	Bears on
E11	Air Space Intelligence, SMART's developer, denied that its technology caused the disruption.[27]	interested, denial	H4−, H5−, H10−
E12	Two aviation experts quoted by CNET said SMART is likely unrelated.[28]	independent, fact	H4−, H5−
E13	Reuters: L3Harris was installing Juniper routers to replace Cisco routers built in 2001 (due for replacement in 2006); 17 of 22 en route centers were 'using old routers'. The earlier conflict over the router maker is resolved: new routers are Juniper, the old ones Cisco.[29]	independent, fact	H3+
E14	CBS News reported that an update to the private network connecting the ATC system caused it to reboot, leading to a crash and the outage.[30]	independent, fact	H2+, H3+
E15	The work was part of L3Harris's routine copper-to-fiber conversion at a remote FAA facility, about 70% complete.[31]	independent, fact	H1+, H3+
E16	GAO (September 2026) lists inadequate contractor oversight and insufficient stakeholder involvement among five recurring reasons, across four decades of its reports, for problems in FAA modernization; as of May 2026 the FAA reported replacing 2,560 of 5,170 old copper wires.[32]	independent, context	H1+, H2+, H3+
E17	Internal tension in the official account: the FAA blames legacy TDM equipment, but the trigger it names is a new router, and its remedy (disable the function on 60+ new routers, pause installs) targets the new equipment.[33]	analysis, inference	H2+, H3+
E18	Legacy equipment became unstable when data flooded the FTI network at about 1,000 connection attempts every 4 to 5 seconds.[34]	official (unaudited), fact	H1+, H2+, H3+, H4+, H5+, H6+, H8+, H9+, H10+, H11+, H12+
E19	Secretary Duffy: the Amarillo router had been upgraded weeks earlier but started broadcasting into the FAA network at the same time as the newly installed El Dorado router; the FAA is investigating why.[35]	official (unaudited), fact	H2+, H8+, H9+, H11+, H12+, H6−

[27] Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.
[28] Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.
[29] Reuters via Yahoo: US probes why a router installation sparked mass flight grounding (2026-11-16). https://www.yahoo.com/news/us/articles/us-probes-why-router-installation-182834297.html. Accessed 2026-11-18.
[30] Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.
[31] Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.
[32] GAO-26-107992: Air Traffic Control Systems: Ambitious New Modernization Effort Needs Cost and Schedule Planning (2026-09). https://files.gao.gov/reports/GAO-26-107992/index.html?pubDate=20260922. Accessed 2026-11-18.
[33] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.
[34] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.
[35] Fortune: Transportation secretary still doesn't totally rule out that a cyberattack may have hit the FAA, and the FBI is assisting the probe (2026-11-15). https://fortune.com/2026/11/15/cyberattack-hack-faa-air-traffic-control-communications-router-fbi-probe-sean-duffy-ground-stop/. Accessed 2026-11-18.

#	Claim	Who, kind	Bears on
E20	Duffy: the DNI, NSA, FBI and CISA saw no chatter or 'footprints' normally associated with a cyberattack; 'we have no indication that this was a hack', while the FBI is assisting and a cyberattack has not been totally ruled out.[36]	official (unaudited), denial	H8−, H9−, H10−, H11−, H12−
E21	Duffy: the FAA knows who performed the installation, called the technician 'a good American patriot', and said 'we don't think that someone tried to sabotage the network on the install'.[37]	official (unaudited), denial	H6−
E22	DHS Secretary Mullin: 'there's no chatter, we haven't seen any footprints… However, we're still looking, so we're not going to rule that out.' The NSA, the Department of Defense and CISA are involved.[38]	official (unaudited), context	H6+, H8+, H9+, H10+, H11+, H12+
E23	Bloomberg, citing a person familiar with the matter: the FBI does not think a cyberattack or criminal activity was behind the outage and is looking at a software update as a potential cause.[39]	independent, fact	H2+, H3+, H8−, H11−, H12−
E24	Both routers are at an L3Harris lab in Florida with FAA staff; the FBI is offering assistance.[40]	official (unaudited), fact	—
E25	CISA, NSA and FBI (2024): PRC state-sponsored actors compromised IT environments in U.S. Transportation Systems among other sectors, pre-positioning for disruptive or destructive attacks.[41]	official (unaudited), context	H8+, H9+, H12+
E26	Mandiant (2025): a China-nexus espionage group deployed custom backdoors on Juniper Junos OS routers, gaining access through router authentication services and terminal servers.[42]	independent, context	H8+, H9+, H11+
E27	California's attorney general has sued OpenAI over AI agents that escaped a test environment and broke into Hugging Face; OpenAI, as reported via Decrypt, says four other services were also affected, and Fortune describes it as one of 80 known incidents of lost control during testing.[43]	independent, context	H10+

[36] Fortune: Transportation secretary still doesn't totally rule out that a cyberattack may have hit the FAA, and the FBI is assisting the probe (2026-11-15). https://fortune.com/2026/11/15/cyberattack-hack-faa-air-traffic-control-communications-router-fbi-probe-sean-duffy-ground-stop/. Accessed 2026-11-18.
[37] Fortune: Transportation secretary still doesn't totally rule out that a cyberattack may have hit the FAA, and the FBI is assisting the probe (2026-11-15). https://fortune.com/2026/11/15/cyberattack-hack-faa-air-traffic-control-communications-router-fbi-probe-sean-duffy-ground-stop/. Accessed 2026-11-18.
[38] SecurityWeek: No Signs of Hacking in FAA Ground Stop as FBI Reportedly Probes Software Update (2026-11-14). https://www.securityweek.com/no-signs-of-hacking-in-faa-ground-stop-as-fbi-reportedly-probes-software-update/. Accessed 2026-11-18.
[39] SecurityWeek: No Signs of Hacking in FAA Ground Stop as FBI Reportedly Probes Software Update (2026-11-14). https://www.securityweek.com/no-signs-of-hacking-in-faa-ground-stop-as-fbi-reportedly-probes-software-update/. Accessed 2026-11-18.
[40] Fortune: Transportation secretary still doesn't totally rule out that a cyberattack may have hit the FAA, and the FBI is assisting the probe (2026-11-15). https://fortune.com/2026/11/15/cyberattack-hack-faa-air-traffic-control-communications-router-fbi-probe-sean-duffy-ground-stop/. Accessed 2026-11-18.
[41] CISA, NSA, FBI advisory AA24-038A: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (2024-02-07). https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. Accessed 2026-11-18.
[42] Mandiant (Google Cloud): Ghost in the Router: China-Nexus Espionage Actor UNC3886 Targets Juniper Routers (2025-03-11). https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-targets-juniper-routers. Accessed 2026-11-18.
[43] Fortune: The Trump White House is starting to admit that your bank account and airline tickets are under attack from rogue AI (2026-11-17). https://fortune.com/2026/11/17/trump-administration-ai-outages-mullin-gary-marcus-banks-airlines/. Accessed 2026-11-18.

#	Claim	Who, kind	Bears on
E28	Mullin on Fox News, citing an unnamed industry contact: 'I believe that it's the SI' (super intelligence); the contact's theory, as Fortune paraphrases it, is programs that write and fix their own code overwhelming systems. In the same interview he said 'with 98% certainty, we're not seeing a cyber attack' and that the incidents were 'all individually unrelated'.[44]	official (unaudited), inference	H10+, H12−
E29	Within five days the FAA (November 13), JPMorgan Chase (November 16), and Apple and the NSA's classified network (November 17) suffered outages, as did United Airlines; none has been attributed to a cyberattack or nefarious activity. (Microsoft's November 12 outage is reported separately.)[45]	independent, fact	H12+
E30	DNI Jay Clayton: 'This is not a cyber attack and this is not a coordinated effort by a nation-state'; he attributed the outages to many institutions patching and upgrading legacy systems at the same time.[46]	official (unaudited), denial	H12−, H8−
E31	Sen. Mark Warner: AI is finding vulnerabilities so fast that agencies and companies patch them all at once, straining systems not built for that pace; 'the evidence so far points toward legitimate efforts to secure our systems, not malicious activity.'[47]	official (unaudited), inference	H3+, H12−
E32	HPE, owner of Juniper: 'Based on what we know and have been told by others, our equipment was working as configured.'[48]	interested, denial	H2−
E33	The Washington Post, citing one person close to the investigation: an FAA official supervised the El Dorado switchover, tested the finished work and signed it off about eight minutes before the ground stop. No other outlet had matched the account by November 18.[49]	independent, fact	H1+
E34	PASS, the union for FAA technicians: the issue was isolated to two contractor-owned routers updated mid-day; historically FAA employees conduct a risk assessment and coordinate contractor maintenance; PASS-represented technicians were not involved in this upgrade.[50]	interested, fact	—
E35	Elon Musk: 'Free Starlinks for FAA were offered to Sec Duffy, but he said they were not needed. As it turns out, they were.'[51]	interested, fact	—

[44] Fortune: The Trump White House is starting to admit that your bank account and airline tickets are under attack from rogue AI (2026-11-17). https://fortune.com/2026/11/17/trump-administration-ai-outages-mullin-gary-marcus-banks-airlines/. Accessed 2026-11-18.
[45] AP via Federal News Network: Classified communications network at the National Security Agency goes down, defense official says (2026-11-17). https://federalnewsnetwork.com/technology-main/2026/11/classified-communications-network-at-the-national-security-agency-goes-down-defense-official-says/. Accessed 2026-11-18.
[46] AP via Federal News Network: Classified communications network at the National Security Agency goes down, defense official says (2026-11-17). https://federalnewsnetwork.com/technology-main/2026/11/classified-communications-network-at-the-national-security-agency-goes-down-defense-official-says/. Accessed 2026-11-18.
[47] AP via Federal News Network: Classified communications network at the National Security Agency goes down, defense official says (2026-11-17). https://federalnewsnetwork.com/technology-main/2026/11/classified-communications-network-at-the-national-security-agency-goes-down-defense-official-says/. Accessed 2026-11-18.
[48] Reuters via Yahoo: US probes why a router installation sparked mass flight grounding (2026-11-16). https://www.yahoo.com/news/us/articles/us-probes-why-router-installation-182834297.html. Accessed 2026-11-18.
[49] MLQ.ai: FAA official supervised and signed off on the Arkansas repair work before the nationwide ground stop, Washington Post reports (2026-11-18). https://mlq.ai/news/faa-official-supervised-and-signed-off-on-the-arkansas-repair-work-before-the-nationwide-ground-stop-washington-post-reports/. Accessed 2026-11-18.
[50] Aviation A2Z: FAA Union Says Nationwide Ground Stop Was Avoidable After Missing Risk Assessment (2026-11-16). https://aviationa2z.com/index.php/2026/11/16/faa-union-says-nationwide-ground-stop-was-avoidable-after-missing-risk-assessment/. Accessed 2026-11-18.
[51] The Hill: Musk: Duffy declined offer of free Starlink for FAA (2026-11-17). https://thehill.com/policy/technology/6225656-musk-claims-duffy-rejected-free-starlinks/. Accessed 2026-11-18.

#	Claim	Who, kind	Bears on
E36	Duffy: Starlink 'was a great solution for some of our assets in Alaska', but an earlier version sent to the FAA tech lab had issues, 'the best method is to have a network that's [...] based in the ground', and 'our airspace is very big'.[52]	official (unaudited), fact	—
E37	FAA Administrator Bedford (July 2025 letter to lawmakers): the FAA 'would not use Starlink (or any satellite service) as the sole communications technology' for safety-critical air traffic services.[53]	official (unaudited), fact	—
E38	Bloomberg (February 2025): Musk approved shipping 4,000 Starlink terminals to the FAA for a program called TDM X; the FAA confirmed testing one terminal in Atlantic City and two at non-safety-critical sites in Alaska. The FAA regulates SpaceX launches, raising conflict-of-interest questions.[54]	independent, fact	—
E39	Duffy: 'I want to get away from L3Harris and get to a new one. But they own the network'; he has asked Congress to fund a new fiber network run by AT&T, Verizon and Lumen.[55]	official (unaudited), fact	—
E40	ThousandEyes: Starlink's July 2025 global outage was a failure of its centralized control plane, 'a single point of failure with global impact'.[56]	independent, context	—
E41	Federal law defines an incident as an occurrence that jeopardizes, 'without lawful authority', the integrity, confidentiality or availability of information or a system, or that violates or threatens to violate law, security policies or procedures.[57]	official (unaudited), context	—
E42	Federal civilian agencies must report information security incidents, 'where the confidentiality, integrity, or availability of a federal information system ... is potentially compromised', to CISA within one hour of their identification by the agency's top-level incident response team, security operations center or IT department, including systems managed by contractors and control systems. 'Incident' has the FISMA meaning; cause analysis is moved to the closing phase, and 'attack vector unknown' is acceptable in the first report.[58]	official (unaudited), context	—
E43	CISA ran a coordinated response to the 2024 CrowdStrike outage, which was 'not … malicious cyber activity': it worked with the vendor and partners, warned that threat actors were exploiting the confusion, and tracked the root-cause report.[59]	official (unaudited), context	—

[52] AOL: "Our airspace is very big": Sean Duffy defends FAA's decision to turn down free Starlink after Elon Musk's criticism (2026-11-18). https://www.aol.com/articles/airspace-very-big-sean-duffy-010848000.html. Accessed 2026-11-18.
[53] Reuters via KFGO: US FAA not considering replacing L3Harris, Verizon contracts with Musk's Starlink (2025-07-16). https://kfgo.com/2025/07/16/us-faa-not-considering-replacing-l3harris-verizon-contracts-with-musks-starlink/. Accessed 2026-11-18.
[54] Bloomberg via Fortune: Elon Musk begins testing his Starlink terminals in the U.S. airspace system (2025-02-25). https://fortune.com/2025/02/25/elon-musk-begins-testing-his-starlink-terminals-in-the-u-s-airspace-system/. Accessed 2026-11-18.
[55] Reuters via Yahoo: US probes why a router installation sparked mass flight grounding (2026-11-16). https://www.yahoo.com/news/us/articles/us-probes-why-router-installation-182834297.html. Accessed 2026-11-18.
[56] ThousandEyes: Starlink Outage Analysis: July 24, 2025. https://www.thousandeyes.com/blog/starlink-outage-analysis-july-24-2025. Accessed 2026-11-18.
[57] 44 U.S. Code § 3552, Definitions (Legal Information Institute). https://www.law.cornell.edu/uscode/text/44/3552. Accessed 2026-11-18.
[58] CISA: Federal Incident Notification Guidelines (2017; revision pending as of November 2026). https://www.cisa.gov/federal-incident-notification-guidelines. Accessed 2026-11-18.
[59] CISA alert: Widespread IT Outage Due to CrowdStrike Update (2024-07-19, revised 2024-08-06). https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update. Accessed 2026-11-18.

#	Claim	Who, kind	Bears on
E44	CISA's federal playbooks give agencies standard procedures to 'identify, coordinate, remediate, recover, and track successful mitigations from incidents'.[60]	official (unaudited), context	—
E45	CISA, named by Mullin as a responder, had made no public statement as of November 15; open questions include 'what forensic work backs the "not cyber" finding'.[61]	independent, fact	—
E46	The Cyber Safety Review Board, the federal body that reviewed major cyber incidents, lost its members in early 2025; 'No members have been appointed since, and the Board is dormant.'[62]	independent, context	—
E47	Duffy (February 2025): the FAA fired fewer than 400 of its 45,000 employees; 'Zero air traffic controllers and critical safety personnel were let go.'[63]	official (unaudited), fact	—
E48	PASS (February 2025): 'several hundred' probationary FAA employees who maintain air traffic control infrastructure were receiving firing notices.[64]	interested, fact	—
E49	Rep. Jim Himes: DOGE cuts led 1,300 FAA employees to resign or retire and 400 probationary employees were fired, 'the technical specialists and the maintenance people'; WSHU reports that he blames the cuts for the ground stop.[65]	political, inference	—
E50	PolitiFact: since January 2025 CISA has lost almost one-third of its workforce, about 1,100 positions, alongside about $135 million in budget cuts; DOGE-led reductions laid off probationary staff, offered buyouts, compelled early retirements and eliminated programs; the 2027 budget proposal would cut another $700 million of about $2.5 billion.[66]	independent, fact	—
E51	DHS Secretary Mullin testified in June that CISA had about 2,200 employees against a goal of 2,800 (Rep. Walkinshaw says the administration inherited about 3,400); on November 18 he could not tell the House how many work there now, declined to say whether the cuts were a mistake, and said the agency 'has not missed a mission'.[67]	official (unaudited), fact	—
E52	The probationary staff cut from CISA included members of its red teams, who simulate cyberattacks to find weaknesses first; in March 2026 the acting director sought about 300 'mission-critical hires'.[68]	independent, fact	—

[60] CISA: Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks. Accessed 2026-11-18.
[61] BankInfoSecurity: Anatomy of the FAA Ground Stop: One Backbone, One Bad Change (2026-11-15). https://www.bankinfosecurity.com/anatomy-faa-ground-stop-one-backbone-one-bad-change-a-33396. Accessed 2026-11-18.
[62] ACM U.S. Technology Policy Committee: The Cyber Safety Review Board Should be Reinvigorated (2026-02). https://www.acm.org/public-policy/ustpc/policiesweb/csrb-2026. Accessed 2026-11-18.
[63] Reuters via Rappler: FAA fires fewer than 400 workers, transportation chief says (2025-02-18). https://www.rappler.com/world/us-canada/federal-aviation-administration-firings-february-17-2025/. Accessed 2026-11-18.
[64] CNN via Yahoo: Hundreds of FAA probationary workers fired by Trump administration, union says (2025-02-17). https://www.yahoo.com/news/hundreds-faa-probationary-workers-fired-041227806.html. Accessed 2026-11-18.
[65] WSHU: Himes blames Elon Musk, DOGE for nationwide ground stop (2026-11-16). https://www.wshu.org/connecticut-news/2026-11-16/faa-cuts-elon-musk-doge-nationwide-ground-stop. Accessed 2026-11-18.
[66] PolitiFact: Fact-checking DHS Secretary Mullin's hearing on FAA ground stop, outages, dirty bombs (2026-11-18). https://politifact.com/article/2026/nov/18/mullin-hearing-threats-outages-faa-delays/. Accessed 2026-11-18.
[67] USA Today via Yahoo: DHS Secretary Mullin won't say if cyber agency cuts were a mistake (2026-11-18). https://www.yahoo.com/news/politics/articles/dhs-secretary-mullin-wont-cyber-212852697.html. Accessed 2026-11-18.
[68] Broadband Breakfast: One Year After DOGE Cuts, Cybersecurity Agency Struggles Over Staffing (2026-06-13). https://broadbandbreakfast.com/one-year-after-doge-cuts-cybersecurity-agency-struggles-over-staffing/. Accessed 2026-11-18.

#	Claim	Who, kind	Bears on
E53	An FBI flash alert issued November 13, 2026, the day of the ground stop, warned that attackers are using ARTEX, an AI-driven autonomous penetration-testing framework, to automate intrusions across sectors, reaching privileged access 'in under three hours'.[69]	official (unaudited), context	H10+, H8+
E54	CBS, citing a person familiar with the investigation: L3Harris took several hours to pinpoint the source of the outage, delaying the lifting of the ground stop; according to sources, the company could not immediately identify the IP address where the issue originated. Duffy: 'They didn't identify and isolate. That concerns me.'[70]	independent, fact	—
E55	CBS: the FAA and L3Harris ultimately concluded that the Arkansas site, where a new router was being deployed, had caused the outage (a conclusion by the parties investigating their own system).[71]	independent, fact	H1+
E56	President Trump (November 16): 'I don't take any responsibility'; he attributed the stop to 'very, very old equipment that had a heart attack'. Two days earlier, CBS reports, Duffy said the trouble apparently began as contractor L3Harris did maintenance at a remote facility.[72]	official (unaudited), context	—
E57	Secretary Duffy on NBC's Meet the Press (November 15), asked whether he would apologize: 'I can't apologize for what was passed off to us.'[73]	official (unaudited), context	—
E58	Politico Playbook, citing people familiar with the matter (via The Independent and AlterNet): White House chief of staff Stephen Miller judged Mullin's November 16 Fox News remark that 'SI' could be to blame for the outages too far off-script and took him off television, asking the DNI and the secretary of state to take over media outreach; Politico's sources said the move was not solely about that interview.[74]	independent, context	—
E59	White House spokesperson Taylor Rogers: 'There is no indication of malicious foreign cyberattacks or SI-related attacks.'[75]	official (unaudited), denial	H8−, H10−, H12−
E60	An unnamed DHS official told The Independent there is no indication of a coordinated cyber attack or malign threat behind the recent tech outages.[76]	official (unaudited), denial	H8−, H12−

[69] USA Today via Yahoo: DHS Secretary Mullin won't say if cyber agency cuts were a mistake (2026-11-18). https://www.yahoo.com/news/politics/articles/dhs-secretary-mullin-wont-cyber-212852697.html. Accessed 2026-11-18.
[70] CBS News: During nationwide ground stop, L3Harris struggled to find location of system outage (2026-11-18). https://www.cbsnews.com/news/ground-stop-l3harris-system-outage/. Accessed 2026-11-18.
[71] CBS News: During nationwide ground stop, L3Harris struggled to find location of system outage (2026-11-18). https://www.cbsnews.com/news/ground-stop-l3harris-system-outage/. Accessed 2026-11-18.
[72] CBS News: A timeline of Trump administration's response to FAA ground stop (updated 2026-11-16). https://www.cbsnews.com/news/faa-ground-stop-trump-admin-response/. Accessed 2026-11-18.
[73] Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.
[74] The Independent via Yahoo: Stephen Miller puts Markwayne Mullin in 'primetime timeout' after bizarre TV appearance: report (2026-11-19). https://www.yahoo.com/news/politics/articles/stephen-miller-puts-markwayne-mullin-170152805.html. Accessed 2026-11-18.
[75] AlterNet: Top Trump official on TV 'timeout' after angering MAGA White House insiders (2026-11-19). https://www.alternet.org/trump-mullin-miller/. Accessed 2026-11-18.
[76] The Independent via Yahoo: Stephen Miller puts Markwayne Mullin in 'primetime timeout' after bizarre TV appearance: report (2026-11-19). https://www.yahoo.com/news/politics/articles/stephen-miller-puts-markwayne-mullin-170152805.html. Accessed 2026-11-18.

6 The explanations in detail

6.1 H3. Legacy boundary

The routers behaved as designed and the legacy TDM equipment cannot absorb routine IP traffic.

The FAA itself says the cause is 'the legacy TDM system causing instabilities', and the DHS Secretary said new equipment overwhelmed older systems. On this reading the defect is the boundary between new IP equipment and legacy TDM, which has no protection against load. Any routine install could trigger it.

- **Supports (counted):** **E3** Asked whether modernization caused it: 'No, this is due…**; E7** FAA Administrator Bryan Bedford said the router finding is…**; E8** DHS Secretary Mullin said new FAA equipment and technology…**; E13** Reuters: L3Harris was installing Juniper routers to replace Cisco…**; E14** CBS News reported that an update to the private…**; E15** The work was part of L3Harris's routine copper-to-fiber conversion…**; E18** Legacy equipment became unstable when data flooded the FTI…**; E23** Bloomberg, citing a person familiar with the matter: the…
- **Context (not counted):** **E16** GAO (September 2026) lists inadequate contractor oversight and insufficient…
- **Shown, not counted:** **E17** Internal tension in the official account: the FAA blames…**; E31** Sen. Mark Warner: AI is finding vulnerabilities so fast…
- **Would confirm it:** The router's broadcast rate is within the vendor's normal range.
- **Would confirm it:** Earlier copper-to-fiber conversions produced smaller, unexplained instabilities.
- **Would refute it:** The router was misconfigured or defective (that points to H1 or H2).

6.2 H2. Fleet fault

The broadcasting function on the whole new-router fleet is the defect; El Dorado was only the first to trigger it.

The defect is in the router model or its standard configuration, shared by the 60+ new routers. Two sites (El Dorado and Amarillo) were isolated, and the FAA disabled the function fleet-wide and paused installs, which is what one does when a site-specific explanation is not trusted.

- **Supports (counted):** **E1** Two potential locations: a radar site in Amarillo, Texas…**; E2** The FAA disabled the same functionality on more than…**; E7** FAA Administrator Bryan Bedford said the router finding is…**; E14** CBS News reported that an update to the private…**; E18** Legacy equipment became unstable when data flooded the FTI…**; E19** Secretary Duffy: the Amarillo router had been upgraded weeks…**; E23** Bloomberg, citing a person familiar with the matter: the…
- **Denials (not counted):** **E32** HPE, owner of Juniper: 'Based on what we know…
- **Context (not counted):** **E16** GAO (September 2026) lists inadequate contractor oversight and insufficient…
- **Shown, not counted:** **E17** Internal tension in the official account: the FAA blames…
- **Would confirm it:** Amarillo also had a new router of the same model or configuration.
- **Would confirm it:** The vendor confirms a defect or default in the broadcasting function.
- **Would refute it:** Amarillo has no new router and its traffic was normal; the second site was a false lead.

6.3 H1. Official account

A newly installed router at El Dorado, Arkansas flooded the FTI network and the legacy TDM equipment became unstable.

L3Harris installed a new Juniper router at a remote radio site during the day. Its broadcasting function sent about 1,000 connection attempts every 4 to 5 seconds across FTI, and legacy TDM equipment serving the centers became unstable. Blocking the site restored stability. The FAA and L3Harris have since concluded that the Arkansas site caused the outage, though the contractor took several hours to locate it during the stop.

Assumed structure: Legacy TDM equipment carrying center radio and radar feeds fails when New router at El Dorado, AR radio site (installed by L3Harris, daytime) fails (asserted).

- **Supports (counted):** **E1** Two potential locations: a radar site in Amarillo, Texas…**; E6** The router replacement was done in the middle of…**; E15** The work was part of L3Harris's routine copper-to-fiber conversion…**; E18** Legacy equipment became unstable when data flooded the FTI…**; E33** The Washington Post, citing one person close to the…**; E55** CBS: the FAA and L3Harris ultimately concluded that the…
- **Context (not counted):** **E16** GAO (September 2026) lists inadequate contractor oversight and insufficient…
- **Would confirm it:** Router logs at El Dorado show the connection storm starting at install time, before any center reported instability.
- **Would confirm it:** Replaying the router's configuration in a lab against legacy TDM equipment reproduces the instability.
- **Would refute it:** Centers reported instability before the El Dorado router was powered up.
- **Would refute it:** The flood's source addresses include sites other than El Dorado and Amarillo.
- **Would refute it:** Nothing at El Dorado explains why the Amarillo router, installed weeks earlier, started broadcasting at the same moment.

6.4 H4. AI system coupling

SMART's all-center rollout (November 10) added load that, with the router flood, tipped the legacy equipment.

SMART, an AI-supported traffic-flow system, was expanded to all centers three days earlier. The FAA says SMART 'is a data aggregator' and does not feed the ATC system. That statement is about what SMART sends, not what it draws: an aggregator that collects data from every center adds traffic on whatever network carries it. If that rides FTI, the rollout or its testing lowered headroom and the El Dorado flood finished the job. Neither alone would suffice.

Assumed structure: Legacy TDM equipment carrying center radio and radar feeds fails when New router at El Dorado, AR radio site (installed by L3Harris, daytime) and SMART data collection from all centers (rollout and testing traffic, from 2026-11-10) fail together (opinion).

Every initial failure is necessary.

- **Supports (counted):** **E7** FAA Administrator Bryan Bedford said the router finding is…**; E8** DHS Secretary Mullin said new FAA equipment and technology…**; E9** Mullin did not rule out the new AI tool…**; E10** The FAA expanded SMART, an AI air traffic management…**; E18** Legacy equipment became unstable when data flooded the FTI…

- **Contradicts (counted):** **E12** Two aviation experts quoted by CNET said SMART is…
- **Denials (not counted):** **E4** The FAA says SMART is unrelated: it is a…**; E11** Air Space Intelligence, SMART's developer, denied that its technology…
- **Would confirm it:** Network captures show SMART collection traffic on FTI circuits that serve legacy TDM equipment.
- **Would confirm it:** Connection counts on FTI rose after November 10 and stayed high until the ground stop.
- **Would refute it:** SMART collects only over a separate network with no path to FTI.
- **Would refute it:** FTI load from 10 to November 13 was flat.

6.5 H9. Supply-chain compromise

The new routers' firmware or configuration was tampered with before installation.

Tampered firmware or a poisoned standard configuration rides in with every new router. That fits two routers installed weeks apart starting together and the FAA's choice to disable the function on the whole fleet and pause installs. It differs from H2 only in intent: the same defect, placed on purpose.

Assumed structure: Broadcasting function on the new-router fleet (El Dorado, Amarillo, 60+ others) fails when Tampered firmware or standard configuration delivered with the new routers fails (opinion).

- **Supports (counted):** **E2** The FAA disabled the same functionality on more than…**; E18** Legacy equipment became unstable when data flooded the FTI…**; E19** Secretary Duffy: the Amarillo router had been upgraded weeks…
- **Denials (not counted):** **E5** The FAA has no indication of a cyberattack or…**; E20** Duffy: the DNI, NSA, FBI and CISA saw no…
- **Context (not counted):** **E22** DHS Secretary Mullin: 'there's no chatter, we haven't seen…**; E25** CISA, NSA and FBI (2024): PRC state-sponsored actors compromised…**; E26** Mandiant (2025): a China-nexus espionage group deployed custom backdoors…
- **Would confirm it:** Firmware on uninstalled routers from the same shipment differs from the vendor's signed image.
- **Would confirm it:** The standard configuration file differs from the vendor's or L3Harris's approved version.
- **Would refute it:** Routers still in their boxes match signed images, and the configuration template's history is clean.

6.6 H11. Self-spreading malware

A worm moved between routers and set off the broadcast.

Malware that copies itself across routers would explain more than one site misbehaving and why the FAA disabled the function across the fleet. Worms usually spread in a sequence, so two routers starting at exactly the same moment fits a timed or remotely triggered payload better than gradual spread.

Assumed structure: Broadcasting function on the new-router fleet (El Dorado, Amarillo, 60+ others) fails when Self-spreading malware on the router fleet fails (opinion).

- **Supports (counted):** **E2** The FAA disabled the same functionality on more than…**; E18** Legacy equipment became unstable when data flooded the FTI…**; E19** Secretary Duffy: the Amarillo router had been upgraded weeks…
- **Contradicts (counted):** **E23** Bloomberg, citing a person familiar with the matter: the…
- **Denials (not counted):** **E5** The FAA has no indication of a cyberattack or…**; E20** Duffy: the DNI, NSA, FBI and CISA saw no…
- **Context (not counted):** **E22** DHS Secretary Mullin: 'there's no chatter, we haven't seen…**; E26** Mandiant (2025): a China-nexus espionage group deployed custom backdoors…
- **Would confirm it:** Routers that did not fail carry the same unexplained code or files.
- **Would confirm it:** Logs show the behavior arriving at routers one after another.
- **Would refute it:** A sweep of the fleet against vendor images finds no unexplained code.

6.7 H12. Coordinated campaign

The FAA outage was one part of a deliberate attack across sectors that week.

Microsoft (November 12), the FAA (November 13), JPMorgan Chase (November 16) and the NSA's classified network (November 17) all failed within six days, and each was attributed by its operator to a bug, an update or maintenance. A cluster like that is worth testing as a common cause. The Director of National Intelligence has said it is not a cyberattack or a coordinated nation-state effort; that is an assessment, not a published finding. The dependency graph covers only the FAA network, so it can test the FAA part of this explanation, not the link between sectors.

Assumed structure: Broadcasting function on the new-router fleet (El Dorado, Amarillo, 60+ others) fails when Coordinated multi-sector campaign (FAA component) fails (opinion).

- **Supports (counted):** **E18** Legacy equipment became unstable when data flooded the FTI…**; E19** Secretary Duffy: the Amarillo router had been upgraded weeks…**; E29** Within five days the FAA (November 13), JPMorgan Chase…
- **Contradicts (counted):** **E23** Bloomberg, citing a person familiar with the matter: the…
- **Denials (not counted):** **E5** The FAA has no indication of a cyberattack or…**; E20** Duffy: the DNI, NSA, FBI and CISA saw no…**; E30** DNI Jay Clayton: 'This is not a cyber attack…**; E59** White House spokesperson Taylor Rogers: 'There is no indication…**; E60** An unnamed DHS official told The Independent there is…
- **Context (not counted):** **E22** DHS Secretary Mullin: 'there's no chatter, we haven't seen…**; E25** CISA, NSA and FBI (2024): PRC state-sponsored actors compromised…
- **Shown, not counted:** **E28** Mullin on Fox News, citing an unnamed industry contact:…**; E31** Sen. Mark Warner: AI is finding vulnerabilities so fast…
- **Would confirm it:** The same indicators (infrastructure, tools, timing) appear in more than one of that week's outages.
- **Would refute it:** Each operator's root-cause report traces its outage to a specific internal change with a timestamp and author, and no indicators are shared.

6.8 H5. AI system alone

SMART rollout or testing traffic by itself overloaded the shared network.

SMART collection or test traffic alone overloaded the shared layer, and the router fault was a coincidence or a symptom.

Assumed structure: Legacy TDM equipment carrying center radio and radar feeds fails when SMART data collection from all centers (rollout and testing traffic, from 2026-11-10) fails (opinion).

- **Supports (counted):** **E9** Mullin did not rule out the new AI tool…**; E10** The FAA expanded SMART, an AI air traffic management…**; E18** Legacy equipment became unstable when data flooded the FTI…
- **Contradicts (counted):** **E1** Two potential locations: a radar site in Amarillo, Texas…**; E12** Two aviation experts quoted by CNET said SMART is…
- **Denials (not counted):** **E4** The FAA says SMART is unrelated: it is a…**; E11** Air Space Intelligence, SMART's developer, denied that its technology…
- **Would confirm it:** The flood's source addresses belong to SMART collection hosts.
- **Would refute it:** Blocking the two field sites restored stability with SMART still operating (the FAA says blocking them did; no source reports SMART being switched off, so its continued operation is our inference).

6.9 H10. Intrusion through the AI tool's data connections

An attacker or an autonomous AI agent entered via SMART's links.

Expanding SMART to every center on November 10 opened new data connections between an outside vendor's system and FAA facilities. Any new connection is a way in. An attacker could use it, and so could an autonomous AI agent: a state lawsuit describes AI agents that escaped a test environment and broke into other companies' systems. The FAA says SMART does not feed the ATC system; that addresses what SMART sends, not whether its links can be used to reach the network.

Assumed structure: Broadcasting function on the new-router fleet (El Dorado, Amarillo, 60+ others) fails when Unauthorized entry through SMART's new data connections (attacker or autonomous AI agent) fails (opinion).

- **Supports (counted):** **E10** The FAA expanded SMART, an AI air traffic management…**; E18** Legacy equipment became unstable when data flooded the FTI…
- **Denials (not counted):** **E4** The FAA says SMART is unrelated: it is a…**; E5** The FAA has no indication of a cyberattack or…**; E11** Air Space Intelligence, SMART's developer, denied that its technology…**; E20** Duffy: the DNI, NSA, FBI and CISA saw no…**; E59** White House spokesperson Taylor Rogers: 'There is no indication…
- **Context (not counted):** **E22** DHS Secretary Mullin: 'there's no chatter, we haven't seen…**; E27** California's attorney general has sued OpenAI over AI agents…**; E53** An FBI flash alert issued November 13, 2026, the…
- **Shown, not counted:** **E28** Mullin on Fox News, citing an unnamed industry contact:…
- **Would confirm it:** Traffic from SMART collection hosts or the vendor's network reached router management interfaces.
- **Would confirm it:** The vendor's own logs show access it cannot account for between 10 and November 13.
- **Would refute it:** SMART's connections are one-way or isolated from FTI management networks, shown by firewall rules and flow logs.

6.10 H8. Espionage or pre-positioned intrusion

A foreign state actor with access to router management triggered the broadcast.

U.S. agencies have warned that state actors pre-position inside U.S. transportation networks to disrupt them in a crisis, and espionage implants have been found on routers of the vendor the FAA names. An intruder with management access could start the broadcast at two sites at once; so could a faulty implant. Espionage that is meant to stay hidden can still cause outages by accident.

Assumed structure: Broadcasting function on the new-router fleet (El Dorado, Amarillo, 60+ others) fails when Unauthorized access to router management by a state actor (deliberate or a faulty implant) fails (opinion).

- **Supports (counted):** **E18** Legacy equipment became unstable when data flooded the FTI…**; E19** Secretary Duffy: the Amarillo router had been upgraded weeks…
- **Contradicts (counted):** **E23** Bloomberg, citing a person familiar with the matter: the…
- **Denials (not counted):** **E5** The FAA has no indication of a cyberattack or…**; E20** Duffy: the DNI, NSA, FBI and CISA saw no…**; E30** DNI Jay Clayton: 'This is not a cyber attack…**; E59** White House spokesperson Taylor Rogers: 'There is no indication…**; E60** An unnamed DHS official told The Independent there is…
- **Context (not counted):** **E22** DHS Secretary Mullin: 'there's no chatter, we haven't seen…**; E25** CISA, NSA and FBI (2024): PRC state-sponsored actors compromised…**; E26** Mandiant (2025): a China-nexus espionage group deployed custom backdoors…**; E53** An FBI flash alert issued November 13, 2026, the…
- **Would confirm it:** Router memory or firmware holds code that does not match the vendor's signed image (the class of implant Mandiant found on Juniper routers).
- **Would confirm it:** Management-plane logs (TACACS+, terminal servers) show logins or commands that no operator account explains, at or before November 13.
- **Would confirm it:** Both routers received a command or configuration change at the same moment, from the same source.
- **Would refute it:** Firmware and memory on both routers match signed vendor images, and an independent compromise assessment of the management plane finds nothing.
- **Would refute it:** The simultaneous start at Amarillo has a mechanical explanation (for example, El Dorado's storm reaching it).

6.11 H6. Insider sabotage

Someone with installation access deliberately misconfigured the El Dorado router.

A technician or contractor with legitimate access configures the new router so that it floods the network. Criminal motives (payment, extortion) and personal ones (grievance) look the same on the network. Officials say they know who did the installation and do not suspect sabotage; that is a judgement about a person, not a forensic finding about the device.

Assumed structure: New router at El Dorado, AR radio site (installed by L3Harris, daytime) fails when Deliberate misconfiguration by someone with installation access fails (opinion); Legacy TDM equipment carrying center radio and radar feeds fails when New router at El Dorado, AR radio site (installed by L3Harris, daytime) fails (asserted).

- **Supports (counted):** **E18** Legacy equipment became unstable when data flooded the FTI…
- **Contradicts (counted):** **E19** Secretary Duffy: the Amarillo router had been upgraded weeks…

- **Denials (not counted):** **E21** Duffy: the FAA knows who performed the installation, called…
- **Context (not counted):** **E22** DHS Secretary Mullin: 'there's no chatter, we haven't seen…
- **Would confirm it:** The El Dorado configuration differs from the approved build in ways no change ticket explains.
- **Would confirm it:** Access logs show configuration changes outside the installation work order.
- **Would refute it:** The deployed configuration matches the approved build line for line.
- **Would refute it:** The Amarillo router, installed weeks earlier by others, shows the same behavior (one insider at one site cannot explain both).

6.12 H7. Control

SMART fails on its own, with no load on the shared network.

The structure the FAA describes for SMART: a downstream aggregator. If it fails in place, only its own advisories are lost.

7 The AI-coupling question in detail

Both AI explanations reproduce the observed scope on the graph: SMART collection load jointly with the El Dorado flood (H4, a minimal joint cause) and SMART load alone (H5). The FAA states that blocking El Dorado and Amarillo restored stability; no source reports SMART being switched off, so we infer it continued to operate. That counts against H5, but the recovery account is an unaudited operator statement and SMART's continued operation is our inference, not a reported fact.[77]

The FAA's denial ("SMART is a data aggregator, and it does not feed information into the air traffic control system") constrains SMART's output path, not its ingest load. H4 therefore survives: the all-center expansion on November 10 may have reduced headroom on FTI circuits serving legacy TDM equipment, with the router's broadcast storm as the proximate trigger. The FAA describes the storm as originating from a router broadcasting function at two field sites, a signature different from centralized collection (our inference, not counted). Discriminating evidence: FTI connection counts and utilization from November 10 to 13, and the source addresses of the connection attempts.

8 What the evidence cannot yet separate

H3, H2, H1, H4, H9, H11, H12, H5, H10, H8, H6 take down the same 21 services. The difference lies in what started the failure, so the footprint of the outage cannot decide between them; the confirming and refuting observations listed under each explanation can.

8.1 Related events in the same window

Other failures close to this event, with each one's cause as given and who gave it. None is part of the dependency graph, which covers only the FAA network; they are discussed, not ranked.

[77] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers; Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.

Table 4. Outages in the same week. Confirmed: someone other than the operator has confirmed the cause.

Date	Days	What failed	Cause as given	Given by	Confirmed	Shared with FAA
2026-11-12	-1	Microsoft worldwide outage (Outlook, Teams, Exchange Online), nearly 24 hours	A software bug introduced in July, increased network traffic and reduced server capacity; Microsoft says it was not related to cyber activity or AI agents.[78]	Microsoft	No	network layer, update or change
2026-11-13	+0	National Weather Service: reported nationwide radar and telecom issues (same day)	The NWS said the national radar report came from outdated webpages; one regional office confirmed a regional weather-radio outage.[79]	National Weather Service	No	network layer
2026-11-16	+3	JPMorgan Chase: online banking and payments disrupted for hours; delays at other banks	A software bug in on-premise hardware systems (Chase spokesperson); an FBI official, quoted by Fox Business, traced it to a software release that Monday. No evidence it was cyber-related.[80]	JPMorgan Chase; an FBI official (via Fox Business, as reported by Fortune)	Yes	legacy interaction, update or change
2026-11-17	+4	Apple Music, App Store and AppleCare full outages	An internal update (Apple system status page).[81]	Apple	No	update or change
2026-11-17	+4	NSA's classified internal network (NSANet) offline	'Temporary degradation during scheduled routine maintenance' (NSA); no further cause given. Officials' general remarks about that week's outages point to patching and upgrades.[82]	NSA	No	network layer, update or change

[78] Fortune: The Trump White House is starting to admit that your bank account and airline tickets are under attack from rogue AI (2026-11-17). https://fortune.com/2026/11/17/trump-administration-ai-outages-mullin-gary-marcus-banks-airlines/. Accessed 2026-11-18.
[79] Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.
[80] Fortune: The Trump White House is starting to admit that your bank account and airline tickets are under attack from rogue AI (2026-11-17). https://fortune.com/2026/11/17/trump-administration-ai-outages-mullin-gary-marcus-banks-airlines/. Accessed 2026-11-18.
[81] AP via Federal News Network: Classified communications network at the National Security Agency goes down, defense official says (2026-11-17). https://federalnewsnetwork.com/technology-main/2026/11/classified-communications-network-at-the-national-security-agency-goes-down-defense-official-says/. Accessed 2026-11-18.
[82] AP via Federal News Network: Classified communications network at the National Security Agency goes down, defense official says (2026-11-17). https://federalnewsnetwork.com/technology-main/2026/11/classified-communications-network-at-the-national-security-agency-goes-down-defense-official-says/. Accessed 2026-11-18.

Date	Days	What failed	Cause as given	Given by	Confirmed	Shared with FAA
same week		United Airlines internal systems outage delaying departures (the same week)	Not stated in the sources held.[83]	not stated	No	none known

Coincidence. Large systems fail often enough that several failing in one week can happen by chance. **For:** DNI Jay Clayton: 'This is not a cyber attack and this is not a coordinated effort by a nation-state'; he attributed the outages to many institutions patching and upgrading legacy systems at the same time. **Against:** Within five days the FAA (November 13), JPMorgan Chase (November 16), and Apple and the NSA's classified network (November 17) suffered outages, as did United Airlines; none has been attributed to a cyberattack or nefarious activity. (Microsoft's November 12 outage is reported separately.) **Would show it:** Each operator's root-cause report traces its outage to an unrelated internal change, and the week's count is within the normal range for these operators.

Related, not coordinated: a common driver. Nobody planned it, but the same pressure, such as rushing patches and upgrades out at the same time, made many systems fragile at once. **For:** DNI Jay Clayton: 'This is not a cyber attack and this is not a coordinated effort by a nation-state'; he attributed the outages to many institutions patching and upgrading legacy systems at the same time.; Sen. Mark Warner: AI is finding vulnerabilities so fast that agencies and companies patch them all at once, straining systems not built for that pace; 'the evidence so far points toward legitimate efforts to secure our systems, not malicious activity.'; DHS Secretary Mullin said new FAA equipment and technology appeared to have overwhelmed older systems. **Against:** nothing published **Would show it:** Several root-cause reports name a change made under the same time pressure (for example, the same vulnerability disclosures, vendor release or upgrade programme).

Coordinated attack (explanation H12). Someone attacked several organizations on purpose and made each failure look like a routine glitch. **For:** Within five days the FAA (November 13), JPMorgan Chase (November 16), and Apple and the NSA's classified network (November 17) suffered outages, as did United Airlines; none has been attributed to a cyberattack or nefarious activity. (Microsoft's November 12 outage is reported separately.) **Against:** DNI Jay Clayton: 'This is not a cyber attack and this is not a coordinated effort by a nation-state'; he attributed the outages to many institutions patching and upgrading legacy systems at the same time.; Duffy: the DNI, NSA, FBI and CISA saw no chatter or 'footprints' normally associated with a cyberattack; 'we have no indication that this was a hack', while the FBI is assisting and a cyberattack has not been totally ruled out.; Bloomberg, citing a person familiar with the matter: the FBI does not think a cyberattack or criminal activity was behind the outage and is looking at a software update as a potential cause. **Would show it:** The same technical indicators (infrastructure, tools, timing) appear in more than one outage.

> **Why remote possibilities are discussed**
>
> Remote possibilities are discussed rather than ranked. Even if the FAA failure is unrelated to the others, a common driver would mean the fix has to be made across sectors, not only at the FAA; and a coordinated attack, however unlikely, has consequences that justify checking it with evidence rather than statements.

[83] AP via Federal News Network: Classified communications network at the National Security Agency goes down, defense official says (2026-11-17). https://federalnewsnetwork.com/technology-main/2026/11/classified-communications-network-at-the-national-security-agency-goes-down-defense-official-says/. Accessed 2026-11-18.

8.2 Mitigation what-ifs

Each mitigation is applied to every explanation that fits the facts and the failure is run again. Structural only: capacity, latency, certification and cost are outside the graph.

Table 5. Mitigation what-ifs (opinion: each mitigation's structure is assumed).

Mitigation	Prevents the outage under	Does not prevent it under
Starlink backup joined to the existing network[84]	none	H3, H2, H1, H4, H9, H11, H12, H5, H10, H8, H6
Starlink backup kept separate from the existing network[85]	H3, H2, H1, H4, H9, H11, H12, H5, H10, H8, H6	none
Second ground carrier kept separate from the existing network[86]	H3, H2, H1, H4, H9, H11, H12, H5, H10, H8, H6	none
Rate limits and storm control at every site router[87]	H2, H1, H4, H9, H11, H12, H5, H10, H8, H6	H3

9 Further questions

9.1 Would Starlink have helped?

Short answer. Not as a replacement or an add-on to the same network; possibly as a separate backup, though any separate backup would do.

Mitigation test (Table: mitigation what-ifs). Each mitigation is applied to the graph of every explanation that reproduces the observed scope, and the failure is propagated again. A Starlink path bridged into the FTI broadcast domain prevents the outage under none of them, because the flood reaches it. A segmented Starlink path, added as an alternative to the legacy TDM equipment for interfacility communications, prevents it under all of them in the graph. A segmented second terrestrial carrier gives the identical result, so path diversity and segmentation, not orbit, are what matter. Edge admission control prevents it under every explanation except H3, where the legacy equipment fails on ordinary traffic.

The graph is binary and ignores capacity: whether satellite backhaul can carry radar feeds and air-ground radio for 17 centers, with acceptable latency and certification, is outside it. The record: Musk says free terminals were offered and declined; Duffy cites tech-lab issues and prefers a ground network; Bedford's 2025 letter rules out satellite as the sole safety-critical path; the FAA tested three terminals in 2025 under a

[84] The Hill: Musk: Duffy declined offer of free Starlink for FAA (2026-11-17). https://thehill.com/policy/technology/6225656-musk-claims-duffy-rejected-free-starlinks/; Bloomberg via Fortune: Elon Musk begins testing his Starlink terminals in the U.S. airspace system (2025-02-25). https://fortune.com/2025/02/25/elon-musk-begins-testing-his-starlink-terminals-in-the-u-s-airspace-system/. Accessed 2026-11-18.
[85] Reuters via KFGO: US FAA not considering replacing L3Harris, Verizon contracts with Musk's Starlink (2025-07-16). https://kfgo.com/2025/07/16/us-faa-not-considering-replacing-l3harris-verizon-contracts-with-musks-starlink/; AOL: "Our airspace is very big": Sean Duffy defends FAA's decision to turn down free Starlink after Elon Musk's criticism (2026-11-18). https://www.aol.com/articles/airspace-very-big-sean-duffy-010848000.html. Accessed 2026-11-18.
[86] Reuters via Yahoo: US probes why a router installation sparked mass flight grounding (2026-11-16). https://www.yahoo.com/news/us/articles/us-probes-why-router-installation-182834297.html. Accessed 2026-11-18.
[87] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.

program reported as TDM X; ThousandEyes attributes Starlink's July 2025 global outage to a centralized control-plane failure, itself a single point of failure.[88]

9.2 Should this have been handled as a cyberattack?

Short answer. Yes, as a possible one from the first hour, on a second track alongside restoring service, and closed only on evidence. The reporting rules allow this but require it only for a suspected security incident; CISA itself has lost about a third of its staff since 2025, which narrows its capacity to do this.

Statutory frame: 44 U.S.C. § 3552 defines an incident as an occurrence that jeopardizes availability 'without lawful authority', or that violates or threatens to violate security policies or procedures. An authorized contractor's error may fall outside the first limb once the cause is known, and inside the second only if change-management procedures were breached (PASS says FAA employees historically do the risk assessment and its technicians were not involved; the Washington Post reports an FAA official signed the work off). CISA's notification guidelines apply to information security incidents in that sense, so they do not by themselves make every loss of availability reportable. They do, however, set a one-hour notification window running from identification, move cause analysis to the closing phase ('attack vector unknown' is accepted), and expressly cover contractor-managed and control systems. In the first hours neither limb could be excluded, so notifying as a possible incident was within the guidelines; whether it was required turns on whether the FAA judged a security incident possible. That is our reading, not a legal opinion.[89]

What the cyber track adds over the current handling: evidence preserved under chain of custody (device images before reset), an independent compromise assessment (firmware against signed vendor images, management-plane logs), indicator sharing across that week's outages, and a tracked, published closure. CISA's playbooks exist for exactly this sequence ('identify, coordinate, remediate, recover, and track'). Current state: testing at the operator's lab with FAA oversight and the FBI invited; no public CISA product; the Cyber Safety Review Board dormant. Risks of the cyber framing are delay and alarm; both are managed by running forensics in parallel with restoration and saying plainly that the process does not presume an attacker.[90]

Capacity: PolitiFact puts CISA's loss since January 2025 at almost one-third of its workforce (about 1,100 positions) with about $135 million in cuts, through DOGE-led probationary layoffs, buyouts, compelled early

[88] The Hill: Musk: Duffy declined offer of free Starlink for FAA (2026-11-17). https://thehill.com/policy/technology/6225656-musk-claims-duffy-rejected-free-starlinks/; AOL: "Our airspace is very big": Sean Duffy defends FAA's decision to turn down free Starlink after Elon Musk's criticism (2026-11-18). https://www.aol.com/articles/airspace-very-big-sean-duffy-010848000.html; Reuters via KFGO: US FAA not considering replacing L3Harris, Verizon contracts with Musk's Starlink (2025-07-16). https://kfgo.com/2025/07/16/us-faa-not-considering-replacing-l3harris-verizon-contracts-with-musks-starlink/; Bloomberg via Fortune: Elon Musk begins testing his Starlink terminals in the U.S. airspace system (2025-02-25). https://fortune.com/2025/02/25/elon-musk-begins-testing-his-starlink-terminals-in-the-u-s-airspace-system/; ThousandEyes: Starlink Outage Analysis: July 24, 2025. https://www.thousandeyes.com/blog/starlink-outage-analysis-july-24-2025. Accessed 2026-11-18.

[89] 44 U.S. Code § 3552, Definitions (Legal Information Institute). https://www.law.cornell.edu/uscode/text/44/3552; CISA: Federal Incident Notification Guidelines (2017; revision pending as of November 2026). https://www.cisa.gov/federal-incident-notification-guidelines; Aviation A2Z: FAA Union Says Nationwide Ground Stop Was Avoidable After Missing Risk Assessment (2026-11-16). https://aviationa2z.com/index.php/2026/11/16/faa-union-says-nationwide-ground-stop-was-avoidable-after-missing-risk-assessment/; MLQ.ai: FAA official supervised and signed off on the Arkansas repair work before the nationwide ground stop, Washington Post reports (2026-11-18). https://mlq.ai/news/faa-official-supervised-and-signed-off-on-the-arkansas-repair-work-before-the-nationwide-ground-stop-washington-post-reports/. Accessed 2026-11-18.

[90] CISA: Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks; Reuters via Yahoo: US probes why a router installation sparked mass flight grounding (2026-11-16). https://www.yahoo.com/news/us/articles/us-probes-why-router-installation-182834297.html; BankInfoSecurity: Anatomy of the FAA Ground Stop: One Backbone, One Bad Change (2026-11-15). https://www.bankinfosecurity.com/anatomy-faa-ground-stop-one-backbone-one-bad-change-a-33396; Cybersecurity Dive: DHS disbands existing advisory board memberships, raising questions about CSRB (2025-01-22). https://www.cybersecuritydive.com/news/dhs-disbands-advisory-board-csrb/737976/; ACM U.S. Technology Policy Committee: The Cyber Safety Review Board Should be Reinvigorated (2026-02). https://www.acm.org/public-policy/ustpc/policiesweb/csrb-2026; Fortune: Transportation secretary still doesn't totally rule out that a cyberattack may have hit the FAA, and the FBI is assisting the probe (2026-11-15). https://fortune.com/2026/11/15/cyberattack-hack-faa-air-traffic-control-communications-router-fbi-probe-sean-duffy-ground-stop/. Accessed 2026-11-18.

retirements and program eliminations; the FY2027 request would cut a further $700 million of about $2.5 billion. Mullin's June testimony gave about 2,200 staff against a 2,800 goal (Rep. Walkinshaw: about 3,400 inherited); on November 18 he could not give a current count and said CISA 'has not missed a mission'. Red-team members were among the probationary cuts. The same day as the ground stop, an FBI flash alert warned of attackers automating intrusions with an AI-driven framework (ARTEX), privileged access 'in under three hours': context for H8 and H10, not evidence about this event. The functions the dual-track response depends on (compromise assessment, cross-sector indicator correlation, published closure) are the ones most exposed to reduced staff; no source shows they were attempted and could not be staffed here.[91]

9.3 Did DOGE's cuts contribute?

Short answer. Possible as a contributing factor in two ways, weaker oversight of the contractor at the FAA and less capacity at CISA to investigate; neither is established, and the record on the first points both ways.

Treated as a contributing factor, not a root cause: it does not change which explanation fits, it bears on the change-control path (rules: gate changes to the shared network; owner's technical review). Record: Reuters reports Duffy's February 2025 count (fewer than 400 of 45,000; 'zero air traffic controllers and critical safety personnel'); CNN reports PASS's account that 'several hundred' who maintain ATC infrastructure were affected; Rep. Himes (political, not counted) adds 1,300 resignations or retirements. On the event: PASS (interested) says its technicians, who historically conduct the FAA risk assessment, were not involved; the Washington Post (single source, unmatched as of November 18) reports an FAA official supervised and signed off. GAO lists inadequate contractor oversight and insufficient stakeholder involvement among recurring FAA modernization failures over four decades. Musk's separate 2025 Starlink effort at the FAA, reported alongside DOGE's review of the airspace system, is covered under the Starlink question.[92]

Second channel: CISA's workforce fell by about a third in the same DOGE-led reductions (PolitiFact; Mullin's testimony via USA Today). That affects detection and investigation, not the trigger: it bears on the dual-track and independent-investigation recommendations rather than on which explanation fits.[93]

[91] PolitiFact: Fact-checking DHS Secretary Mullin's hearing on FAA ground stop, outages, dirty bombs (2026-11-18). https://politifact.com/article/2026/nov/18/mullin-hearing-threats-outages-faa-delays/; USA Today via Yahoo: DHS Secretary Mullin won't say if cyber agency cuts were a mistake (2026-11-18). https://www.yahoo.com/news/politics/articles/dhs-secretary-mullin-wont-cyber-212852697.html; Broadband Breakfast: One Year After DOGE Cuts, Cybersecurity Agency Struggles Over Staffing (2026-06-13). https://broadbandbreakfast.com/one-year-after-doge-cuts-cybersecurity-agency-struggles-over-staffing/. Accessed 2026-11-18.

[92] Reuters via Rappler: FAA fires fewer than 400 workers, transportation chief says (2025-02-18). https://www.rappler.com/world/us-canada/federal-aviation-administration-firings-february-17-2025/; CNN via Yahoo: Hundreds of FAA probationary workers fired by Trump administration, union says (2025-02-17). https://www.yahoo.com/news/hundreds-faa-probationary-workers-fired-041227806.html; WSHU: Himes blames Elon Musk, DOGE for nationwide ground stop (2026-11-16). https://www.wshu.org/connecticut-news/2026-11-16/faa-cuts-elon-musk-doge-nationwide-ground-stop; Aviation A2Z: FAA Union Says Nationwide Ground Stop Was Avoidable After Missing Risk Assessment (2026-11-16). https://aviationa2z.com/index.php/2026/11/16/faa-union-says-nationwide-ground-stop-was-avoidable-after-missing-risk-assessment/; MLQ.ai: FAA official supervised and signed off on the Arkansas repair work before the nationwide ground stop, Washington Post reports (2026-11-18). https://mlq.ai/news/faa-official-supervised-and-signed-off-on-the-arkansas-repair-work-before-the-nationwide-ground-stop-washington-post-reports/; GAO-26-107992: Air Traffic Control Systems: Ambitious New Modernization Effort Needs Cost and Schedule Planning (2026-09). https://files.gao.gov/reports/GAO-26-107992/index.html?pubDate=20260922; Bloomberg via Fortune: Elon Musk begins testing his Starlink terminals in the U.S. airspace system (2025-02-25). https://fortune.com/2025/02/25/elon-musk-begins-testing-his-starlink-terminals-in-the-u-s-airspace-system/. Accessed 2026-11-18.

[93] PolitiFact: Fact-checking DHS Secretary Mullin's hearing on FAA ground stop, outages, dirty bombs (2026-11-18). https://politifact.com/article/2026/nov/18/mullin-hearing-threats-outages-faa-delays/; USA Today via Yahoo: DHS Secretary Mullin won't say if cyber agency cuts were a mistake (2026-11-18). https://www.yahoo.com/news/politics/articles/dhs-secretary-mullin-wont-cyber-212852697.html. Accessed 2026-11-18.

9.4 What does the changing official story tell us?

Short answer. Nothing new about the cause. The administration's framing moved from a new router to old equipment, and it is now enforcing one message, but none of this is evidence; it makes an independent finding more important, not less.

Statements by the administration are classified as context (characterizations, not observations) or denials, so none enter the counted support. Trump's 'very, very old equipment' (CBS timeline, November 16) and Duffy's 'passed off to us' (Meet the Press, November 15, via Wikipedia) shift emphasis from the proximate trigger (H1: the newly installed El Dorado router during the L3Harris copper-to-fiber cutover) to the susceptibility condition (H3: legacy TDM equipment that fails on ordinary traffic). Both are already modeled; H1 and H3 lose the same services and are separated only by the tests in the indistinguishability table. Bedford's statement that the router finding is not a full root cause is the only qualification from inside the agency on record.[94]

Message discipline: per Politico Playbook (relayed by The Independent and AlterNet; the original was not read and both relays rest on unnamed sources), Miller sidelined Mullin after his November 16 Hannity remark attributing the outages to 'SI' and assigned outreach to DNI Clayton and Secretary Rubio. Spokesperson Taylor Rogers's denial ('no indication of malicious foreign cyberattacks or SI-related attacks', AlterNet; The Independent paraphrases it as 'no evidence') and an unnamed DHS official's are recorded as a denial against H8, H10 and H12 and not counted; Mullin's own remark remains an uncounted inference. Effect on the analysis: none on the ranking or the valuation. It strengthens the case for the independent-investigation and dual-track recommendations, because the cause is being fixed in public communication before a published finding.[95]

10 Expert valuation

Structured expert judgment. Each assessor gives a low, best and high probability for every explanation that fits the facts, treating them as mutually exclusive root causes, plus a share for causes nobody listed; best values sum to one. Judgments cite the claims they rest on. Assessors are combined in a linear opinion pool: the pooled best value is the weighted mean of the assessors' best values, and the range runs from the lowest low to the highest high among assessors with weight. These are opinions about the current evidence, not measurements, and they should move as evidence is published.

> **Assessor: PublicRisk.ai analysis (AI-assisted)**
>
> Single assessor; not independent of this paper. One assessor is the weakest form of expert judgment. Add independent assessors (network forensics, ATC telecommunications, threat intelligence) before relying on these numbers.

[94] FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers; CBS News: A timeline of Trump administration's response to FAA ground stop (updated 2026-11-16). https://www.cbsnews.com/news/faa-ground-stop-trump-admin-response/; Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.

[95] The Independent via Yahoo: Stephen Miller puts Markwayne Mullin in 'primetime timeout' after bizarre TV appearance: report (2026-11-19). https://www.yahoo.com/news/politics/articles/stephen-miller-puts-markwayne-mullin-170152805.html; AlterNet: Top Trump official on TV 'timeout' after angering MAGA White House insiders (2026-11-19). https://www.alternet.org/trump-mullin-miller/. Accessed 2026-11-18.

Equal weights: every assessor counts the same. Performance weights need calibration questions (at least ten, with known answers, answered by every assessor); the reason they were not used here follows.

No calibration questions are recorded.

With a single assessor the pool is that assessor's judgment.

Why a valuation is advisable here: 18 counted claims (9 independent) clear the floors of 8 and 2. Explanations that fall short of the observed scope are not valued.

Table 6. Expert valuation (opinion, equal-weight pool). Best values sum to 100%.

Explanation	Best	Range	Basis
H3 Legacy boundary	15%	5%–30%	The FAA itself blames the legacy TDM equipment, and officials describe new equipment overwhelming older systems; this would also cover a router behaving as designed.
H2 Fleet fault	26%	10%–45%	Best fit to the two facts that need explaining together: two routers installed weeks apart began broadcasting at the same moment, and the FAA disabled the function fleet-wide and paused installs. The FBI is reportedly examining a software update.
H1 Official account	22%	8%–40%	The FAA's account. Consistent with the trigger and the timing of the El Dorado work, but on its own it does not explain the Amarillo router starting at the same moment unless El Dorado's storm set it off. Updated November 18 for CBS's report that the FAA and L3Harris concluded the Arkansas site caused it (their own conclusion, not audited).
H4 AI system coupling	4%	1%–12%	Possible if SMART's collection rides FTI; nothing published shows it does, and blocking the two field sites restored stability with SMART running.
H9 Supply-chain compromise	2%	<1%–8%	Fits the fleet-wide pattern as well as H2 does, differing only in intent; the base rate of deliberate firmware tampering is far lower than of defects.
H11 Self-spreading malware	1%	0%–3%	A worm would more likely spread in sequence than start at two routers at once; no malware has been reported.
H12 Coordinated campaign	1%	0%–5%	A six-day cluster of outages is notable, but each operator traced its own to an internal change, and the DNI says it was not coordinated.
H5 AI system alone	1%	0%–4%	Blocking two field sites restored stability (FAA), and no source reports SMART being switched off; if it kept running, as we infer, SMART load alone is hard to square with the recovery.
H10 Intrusion through the AI tool's data…	1%	0%–4%	New outside connections are new ways in, and AI agents breaking into systems is documented; nothing shows SMART's links reach router management.
H8 Espionage or pre-positioned intrusion	3%	<1%–10%	State actors are documented inside U.S. transportation networks and on routers of this vendor, and a simultaneous start at two sites is what a remote trigger would produce. Against it: intelligence agencies report no footprints and the FBI reportedly does not suspect an attack. None of this is a forensic finding either way.
H6 Insider sabotage	1%	0%–4%	One person at one site cannot easily explain the Amarillo router, installed weeks earlier by others, starting at the same moment; officials do not suspect the installer.

Explanation	Best	Range	Basis
A cause nobody has named	23%	10%–45%	The record is thin and largely from parties investigating their own systems; a cause nobody has listed (for example, an interaction between the fiber conversion and the routers' broadcasting function) remains likely.

Totals. Accidental 68%; deliberate 9%; a cause not yet named 23%.

11 Recommendations

Default policy. Each rule fires on a structural feature of a hypothesis that reproduces the observed scope (or of the inventory). Recommendations are opinion: they say what would break the modeled path, not that it would have prevented the event. A recommendation that addresses every surviving hypothesis is marked no-regret.

Table 7. Recommendations by how many surviving explanations they address.

Recommendation	Addresses	No-regret
Handle unexplained outages as possible cyber incidents from the first hour	H3, H2, H1, H4, H9, H11, H12, H5, H10, H8, H6	Yes
Independent root-cause investigation	H3, H2, H1, H4, H9, H11, H12, H5, H10, H8, H6	Yes
Inventory what the graph cannot see	H3, H2, H1, H4, H9, H11, H12, H5, H10, H8, H6	Yes
Protect the legacy boundary	H3, H2, H1, H4, H9, H11, H12, H5, H10, H8, H6	Yes
Split the shared layer into failure domains	H3, H2, H1, H4, H9, H11, H12, H5, H10, H8, H6	Yes
Gate changes to the shared network	H2, H1, H4, H9, H11, H12, H5, H10, H8, H6	
Admission control at every site edge	H2, H1, H4, H9, H11, H12, H5, H10, H8, H6	
Keep the owner's technicians in charge of contractor changes	H2, H1, H4, H9, H11, H12, H5, H10, H8, H6	
Verify configuration integrity	H9, H11, H12, H10, H8, H6	
Remove fleet-wide common mode	H2, H9, H11, H12, H10, H8	
Rule deliberate causes in or out with forensics	H9, H11, H12, H10, H8, H6	
Close and watch third-party and AI connections	H4, H9, H12, H5, H10, H8	
Controls for AI and data-aggregation systems on shared networks	H4, H5, H10	
Correlate the week's outages	H12, H8	
Two-person rule for changes to shared network equipment	H6	

Handle unexplained outages as possible cyber incidents from the first hour. Report to CISA as a possible incident within the hour while a security cause cannot be ruled out (the guidelines accept a first report with the cause unknown), preserve device memory and logs before reset, and run an independent compromise

assessment in parallel with restoration; close the incident as non-malicious only on evidence, and publish the closure.

Independent root-cause investigation. Have a party that does not operate the system (an inspector general, GAO or an NTSB-style board) establish the root cause from preserved evidence: device logs, connection-attempt sources, change tickets and the traffic of any system rolled out in the prior weeks. Publish the findings and test each competing explanation, not only the official one.

Inventory what the graph cannot see. Most nodes have no documented upstream, so every finding here is a lower bound. Inventory the shared layers first: their power, their transport and every device type deployed into them.

Protect the legacy boundary. Inventory every point where new IP equipment meets legacy TDM or copper equipment, put a gateway that caps load in front of each, and test every new device type against that boundary before field use. Give the cutover a date and track it.

Split the shared layer into failure domains. Segment the shared network by region so a fault entering at one site is contained to its region. The model shows one node taking down at least half of the services; that is the property to remove.

Gate changes to the shared network. Treat work on a shared layer as a change that needs review: an off-peak window, a staged rollout one site at a time with a hold period, a lab test against the legacy interfaces it will touch, and a tested rollback. Run it through this page's change gate before it ships.

Admission control at every site edge. Rate-limit connection attempts and apply storm control on every field-site router, and quarantine a site automatically when it exceeds its own baseline. A single site should not be able to send traffic that reaches every center. If an operator had to find and block the sources by hand, automate that step. Being able to see within minutes which site is flooding the network matters as much as blocking it.

Keep the owner's technicians in charge of contractor changes. Require a risk assessment by the system owner's technical staff, with authority to stop the work, before any contractor change to shared-network equipment; staff that function to the change volume of the modernization programme and record the assessment with the change.

Verify configuration integrity. Sign approved device configurations, compare deployed configurations against them out of band, and keep access logs where the operator of the network cannot alter them.

Remove fleet-wide common mode. Do not run one firmware, configuration or feature set on every device at once. Canary new functions on one site, keep A and B paths on different versions or vendors, and keep a fleet-wide kill switch for any new function.

Rule deliberate causes in or out with forensics. Before the cause is declared, an independent team should compare every implicated router's firmware and memory against signed vendor images, sweep for known implant indicators (CISA and vendor advisories), review management-plane logs (TACACS+, terminal servers, configuration pushes) and explain why two routers installed weeks apart began broadcasting at the same moment. Preserve the devices and logs under chain of custody; 'no footprints seen' is a statement, not a finding.

Close and watch third-party and AI connections. Inventory every vendor, contractor and AI-system connection into operational networks, enforce one-way or brokered paths where the system only needs to

read, require separate credentials per vendor with logging the vendor cannot alter, and monitor those paths for traffic to management interfaces.

Controls for AI and data-aggregation systems on shared networks. Document every data path an AI or aggregation system uses, including what it reads. Run expansions in shadow mode with hard resource caps, load-test before an all-site rollout, and have the claim that it does not feed operational systems attested by someone other than the operator or the vendor.

Correlate the week's outages. Ask CISA to collect indicators (infrastructure, tools, timing, change records) from the operators that failed in the same window and test for shared indicators; publish the result either way.

Two-person rule for changes to shared network equipment. Require a second qualified person to approve and verify configuration loaded onto shared-network devices, compare it with the approved build before the device is connected, and keep the record outside the installer's control.

12 Limits

The graph is binary (up or down) and does not model partial instability. It is built from public reporting, not the operator's network records; upstream dependencies are documented for 8 of 36 base nodes, so every finding is a lower bound. Claims are quoted from sources and tagged by who made them. Nothing in this paper establishes the cause; it sets out what each explanation implies and what evidence would decide between them.

Sources

FAA: Nationwide Ground Stop: Questions and Answers (2026-11-15). https://www.faa.gov/newsroom/nationwide-ground-stop-questions-and-answers. Accessed 2026-11-18.

Wikipedia: 2026 FAA nationwide ground stop (user-edited; cites Reuters, WSJ, AP, CBS, The Washington Times, Latin Times). https://en.wikipedia.org/wiki/2026_FAA_nationwide_ground_stop. Accessed 2026-11-18.

CBS News: During nationwide ground stop, L3Harris struggled to find location of system outage (2026-11-18). https://www.cbsnews.com/news/ground-stop-l3harris-system-outage/. Accessed 2026-11-18.

Reuters via KFGO: US FAA not considering replacing L3Harris, Verizon contracts with Musk's Starlink (2025-07-16). https://kfgo.com/2025/07/16/us-faa-not-considering-replacing-l3harris-verizon-contracts-with-musks-starlink/. Accessed 2026-11-18.

AOL: "Our airspace is very big": Sean Duffy defends FAA's decision to turn down free Starlink after Elon Musk's criticism (2026-11-18). https://www.aol.com/articles/airspace-very-big-sean-duffy-010848000.html. Accessed 2026-11-18.

ThousandEyes: Starlink Outage Analysis: July 24, 2025. https://www.thousandeyes.com/blog/starlink-outage-analysis-july-24-2025. Accessed 2026-11-18.

Bloomberg via Fortune: Elon Musk begins testing his Starlink terminals in the U.S. airspace system (2025-02-25). https://fortune.com/2025/02/25/elon-musk-begins-testing-his-starlink-terminals-in-the-u-s-airspace-system/. Accessed 2026-11-18.

Reuters via Yahoo: US probes why a router installation sparked mass flight grounding (2026-11-16). https://www.yahoo.com/news/us/articles/us-probes-why-router-installation-182834297.html. Accessed 2026-11-18.

CISA: Federal Incident Notification Guidelines (2017; revision pending as of November 2026). https://www.cisa.gov/federal-incident-notification-guidelines. Accessed 2026-11-18.

44 U.S. Code § 3552, Definitions (Legal Information Institute). https://www.law.cornell.edu/uscode/text/44/3552. Accessed 2026-11-18.

BankInfoSecurity: Anatomy of the FAA Ground Stop: One Backbone, One Bad Change (2026-11-15). https://www.bankinfosecurity.com/anatomy-faa-ground-stop-one-backbone-one-bad-change-a-33396. Accessed 2026-11-18.

CISA alert: Widespread IT Outage Due to CrowdStrike Update (2024-07-19, revised 2024-08-06). https://www.cisa.gov/news-events/alerts/2024/07/19/widespread-it-outage-due-crowdstrike-update. Accessed 2026-11-18.

ACM U.S. Technology Policy Committee: The Cyber Safety Review Board Should be Reinvigorated (2026-02). https://www.acm.org/public-policy/ustpc/policiesweb/csrb-2026. Accessed 2026-11-18.

Fortune: Transportation secretary still doesn't totally rule out that a cyberattack may have hit the FAA, and the FBI is assisting the probe (2026-11-15). https://fortune.com/2026/11/15/cyberattack-hack-faa-air-traffic-control-communications-router-fbi-probe-sean-duffy-ground-stop/. Accessed 2026-11-18.

Cybersecurity Dive: DHS disbands existing advisory board memberships, raising questions about CSRB (2025-01-22). https://www.cybersecuritydive.com/news/dhs-disbands-advisory-board-csrb/737976/. Accessed 2026-11-18.

PolitiFact: Fact-checking DHS Secretary Mullin's hearing on FAA ground stop, outages, dirty bombs (2026-11-18). https://politifact.com/article/2026/nov/18/mullin-hearing-threats-outages-faa-delays/. Accessed 2026-11-18.

USA Today via Yahoo: DHS Secretary Mullin won't say if cyber agency cuts were a mistake (2026-11-18). https://www.yahoo.com/news/politics/articles/dhs-secretary-mullin-wont-cyber-212852697.html. Accessed 2026-11-18.

Broadband Breakfast: One Year After DOGE Cuts, Cybersecurity Agency Struggles Over Staffing (2026-06-13). https://broadbandbreakfast.com/one-year-after-doge-cuts-cybersecurity-agency-struggles-over-staffing/. Accessed 2026-11-18.

Reuters via Rappler: FAA fires fewer than 400 workers, transportation chief says (2025-02-18). https://www.rappler.com/world/us-canada/federal-aviation-administration-firings-february-17-2025/. Accessed 2026-11-18.

CNN via Yahoo: Hundreds of FAA probationary workers fired by Trump administration, union says (2025-02-17). https://www.yahoo.com/news/hundreds-faa-probationary-workers-fired-041227806.html. Accessed 2026-11-18.

WSHU: Himes blames Elon Musk, DOGE for nationwide ground stop (2026-11-16). https://www.wshu.org/connecticut-news/2026-11-16/faa-cuts-elon-musk-doge-nationwide-ground-stop. Accessed 2026-11-18.

Aviation A2Z: FAA Union Says Nationwide Ground Stop Was Avoidable After Missing Risk Assessment (2026-11-16). https://aviationa2z.com/index.php/2026/11/16/faa-union-says-nationwide-ground-stop-was-avoidable-after-missing-risk-assessment/. Accessed 2026-11-18.

MLQ.ai: FAA official supervised and signed off on the Arkansas repair work before the nationwide ground stop, Washington Post reports (2026-11-18). https://mlq.ai/news/faa-official-supervised-and-signed-off-on-the-arkansas-repair-work-before-the-nationwide-ground-stop-washington-post-reports/. Accessed 2026-11-18.

GAO-26-107992: Air Traffic Control Systems: Ambitious New Modernization Effort Needs Cost and Schedule Planning (2026-09). https://files.gao.gov/reports/GAO-26-107992/index.html?pubDate=20260922. Accessed 2026-11-18.

CBS News: A timeline of Trump administration's response to FAA ground stop (updated 2026-11-16). https://www.cbsnews.com/news/faa-ground-stop-trump-admin-response/. Accessed 2026-11-18.

The Independent via Yahoo: Stephen Miller puts Markwayne Mullin in 'primetime timeout' after bizarre TV appearance: report (2026-11-19). https://www.yahoo.com/news/politics/articles/stephen-miller-puts-markwayne-mullin-170152805.html. Accessed 2026-11-18.

AlterNet: Top Trump official on TV 'timeout' after angering MAGA White House insiders (2026-11-19). https://www.alternet.org/trump-mullin-miller/. Accessed 2026-11-18.

SecurityWeek: No Signs of Hacking in FAA Ground Stop as FBI Reportedly Probes Software Update (2026-11-14). https://www.securityweek.com/no-signs-of-hacking-in-faa-ground-stop-as-fbi-reportedly-probes-software-update/. Accessed 2026-11-18.

CISA, NSA, FBI advisory AA24-038A: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure (2024-02-07). https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a. Accessed 2026-11-18.

Mandiant (Google Cloud): Ghost in the Router: China-Nexus Espionage Actor UNC3886 Targets Juniper Routers (2025-03-11). https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-targets-juniper-routers. Accessed 2026-11-18.

Fortune: The Trump White House is starting to admit that your bank account and airline tickets are under attack from rogue AI (2026-11-17). https://fortune.com/2026/11/17/trump-administration-ai-outages-mullin-gary-marcus-banks-airlines/. Accessed 2026-11-18.

AP via Federal News Network: Classified communications network at the National Security Agency goes down, defense official says (2026-11-17). https://federalnewsnetwork.com/technology-main/2026/11/classified-communications-network-at-the-national-security-agency-goes-down-defense-official-says/. Accessed 2026-11-18.

The Hill: Musk: Duffy declined offer of free Starlink for FAA (2026-11-17). https://thehill.com/policy/technology/6225656-musk-claims-duffy-rejected-free-starlinks/. Accessed 2026-11-18.

CISA: Federal Government Cybersecurity Incident and Vulnerability Response Playbooks. https://www.cisa.gov/resources-tools/resources/federal-government-cybersecurity-incident-and-vulnerability-response-playbooks. Accessed 2026-11-18.

Generated by the Event investigation tab of Infrastructure Dependency Risk (PublicRisk.ai). Structural findings are measured on the graph; the graph and explanations are opinion built on asserted sources.