United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued April 11, 2025 Decided January 20, 2026

No. 23-1155

SPOKANE AIRPORT BOARD,
PETITIONER

v.

TRANSPORTATION SECURITY ADMINISTRATION,
RESPONDENT

On Petition for Review of a Final Order
of the Transportation Security Administration

James A. McPhee argued the cause for petitioner. With him on the briefs were *Brian M. Werst* and *Jon T. Burtard*.

Ben Lewis, Attorney, U.S. Department of Justice, argued the cause for respondent. With him on the brief were *Brett A. Shumate*, Acting Assistant Attorney General, U.S. Department of Justice, and *Sharon Swingle*, Attorney, U.S. Department of Justice.

Before: SRINIVASAN, *Chief Judge*, RAO and PAN, *Circuit Judges*.

Opinion for the Court filed by *Circuit Judge* RAO.

RAO, *Circuit Judge*: Facing increased cybersecurity threats to the aviation sector, the Transportation Security Administration ("TSA") issued an emergency amendment requiring airport security programs to include certain cybersecurity measures and controls. Spokane Airport Board ("Spokane") petitions for review, arguing that TSA's amendment was without statutory authority, inconsistent with regulatory requirements, and arbitrary and capricious. Several of Spokane's arguments were not raised below, so we cannot consider them, and the remaining arguments fail on the merits. We therefore deny Spokane's petition.

I.

A.

Following the terrorist attacks of September 11, 2001, Congress established TSA and vested it with responsibility for "civil aviation security." Aviation & Transportation Security Act, Pub. L. No. 107-71, § 101(a), 115 Stat. 597, 597 (2001). TSA is required to "assess threats to transportation" and to "develop policies, strategies, and plans for dealing with threats to transportation security." 49 U.S.C. § 114(f)(2)–(3).

As relevant to this case, TSA is specifically required to "oversee the implementation, and ensure the adequacy, of security measures at airports." *Id.* § 114(f)(11). By regulation, airports must adopt and implement "airport security programs" to provide for "the safety and security of persons and property on an aircraft operating in air transportation." 49 C.F.R. § 1542.101(a)(1). Once an airport security program has been approved by TSA, it may be amended upon approval of an airport operator's request or by TSA through notice and comment procedures. *Id.* § 1542.105(b)–(c).

If, however, TSA finds that "an emergency requiring immediate action with respect to safety and security in air transportation" makes the ordinary procedural requirements "contrary to the public interest," TSA may issue an amendment to airport security programs without providing opportunity for public comment. *Id.* § 1542.105(d). For an emergency amendment, TSA must issue a notice that includes a "brief statement of the reasons and findings" justifying the amendment. *Id.* An emergency amendment is immediately effective and is not stayed by the filing of a petition for reconsideration. *Id.*

B.

In recent years, the federal government has become concerned about the aviation sector's vulnerability to cyberattacks. For instance, cybercriminals have repeatedly launched ransomware attacks that disrupt aviation supply chains; a foreign state affiliated actor conducted a cyberespionage campaign against multiple U.S. airports, airlines, and aviation support organizations; and a set of pro-Russia hacktivist groups launched cyberattacks against airport websites. Still other unidentified cyber actors have targeted individual airports and airlines.[1]

In August 2022, TSA responded to this emergent threat by proposing an amendment to the security programs of certain large airports. *See* Proposed Requirement to Amend TSA-Approved Airport Security Program, TSA-PNA-22-03 (Aug. 11, 2022). The proposed amendment would have required covered airports to implement cybersecurity measures to

[1] The government cites classified materials for additional evidence of cybersecurity threats to aviation. We have reviewed this material, but rely only on materials from the public record in this opinion.

protect against foreign adversaries and other malicious actors. The proposed amendment received hundreds of comments from industry participants and other interested parties. Seeking "further discussion," TSA rescinded the proposed amendment in November 2022 and held "additional industry engagement calls." J.A. 73.

A few months later, TSA promulgated an emergency amendment that substantially incorporated the previously proposed amendment. *See* Joint Emergency Amendment to TSA-Approved Security Program, 23-01 (Mar. 7, 2023) (the "Amendment") (relying in relevant part on emergency authority in 49 C.F.R. § 1542.105(d)). The Amendment requires certain airport and aircraft operators to add cybersecurity measures and controls to their security programs. Airport operators must identify a list of critical systems within 30 days of the Amendment's effective date, submit to TSA a Cybersecurity Implementation Plan containing a set of cybersecurity measures and controls for those systems within 90 days of the effective date, and annually assess the effectiveness of their cybersecurity plans. TSA issued the Amendment without notice and comment because it determined that "there is an emergency requiring immediate action" to protect "national and transportation security" from the impact of cybersecurity threats.

Spokane Airport Board, which operates Spokane International Airport in eastern Washington, petitioned TSA for reconsideration. Spokane raised several procedural and substantive objections to the Amendment. TSA rejected the reconsideration petitions of Spokane and other objectors. Spokane filed a timely petition for review. *See* 49 U.S.C. § 46110(a).

II.

We have authority to "affirm, amend, modify, or set aside any part of" a TSA order. 49 U.S.C. § 46110(c). Section 46110 is silent as to the standard of review, and so we apply the standards set forth in the Administrative Procedure Act. *Cf. Carus Chem. Co. v. EPA*, 395 F.3d 434, 441 (D.C. Cir. 2005). TSA's decision will be upheld "unless it is 'arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.'" *Ramsingh v. TSA*, 40 F.4th 625, 631 (D.C. Cir. 2022) (quoting 5 U.S.C. § 706(2)(A)).

An objection to TSA's order may be considered "only if the objection was made in the proceeding" below or there was a "reasonable ground" for failing to raise it. 49 U.S.C. § 46110(d). We have held that an objection not raised or excused is "jurisdictionally barred."[2] *City of Olmsted Falls v. FAA*, 292 F.3d 261, 274 (D.C. Cir. 2002); *see also Wallaesa v. FAA*, 824 F.3d 1071, 1077 n.4 (D.C. Cir. 2016) (holding that section 46110(d)'s bar applies even when not invoked by the government).

III.

Spokane argues the Amendment should be set aside because: (1) TSA lacks statutory authority to regulate cybersecurity; (2) the Amendment is inconsistent with TSA

---

[2] The Supreme Court has indicated that most exhaustion requirements are "claim-processing rule[s]" and "ordinarily … not jurisdictional." *Santos-Zacaria v. Garland*, 143 S. Ct. 1103, 1112 (2023) (cleaned up); *see also EPA v. EME Homer City Generation, LP*, 572 U.S. 489, 511–12 (2014) (holding the Clean Air Act's exhaustion requirement is not jurisdictional). But this court has squarely held that section 46110(d) is jurisdictional, and we follow this controlling precedent.

regulations; (3) the Amendment was required to be, but never was, ratified by the Transportation Security Oversight Board; and (4) the Amendment was arbitrary and capricious. We hold that these arguments either were not properly raised before TSA or fail on the merits.

A.

We begin with Spokane's argument that the Amendment exceeds TSA's statutory authority because the agency is not explicitly empowered to regulate cybersecurity and other statutes address cybersecurity without granting regulatory authority to TSA.

TSA has statutory authority to regulate cybersecurity. Congress has conferred on TSA "broad statutory authority to protect civil aviation security." *Bonacci v. TSA*, 909 F.3d 1155, 1157 (D.C. Cir. 2018); *see* 49 U.S.C. § 114(d)(1). TSA must "assess threats to transportation" and "develop policies, strategies, and plans for dealing with threats to transportation security." 49 U.S.C. § 114(f)(2)–(3). Spokane does not dispute that cyberattacks increasingly pose a threat to transportation security, especially in the aviation sector. And TSA's regulatory mandate allows it to assess and address such "risks to aviation and national security." *Olivares v. TSA*, 819 F.3d 454, 466 (D.C. Cir. 2016). Further, as Spokane acknowledges, Congress has evinced a specific concern for the impact of cyberattacks on aviation, explicitly instructing TSA to "periodically review threats to civil aviation" including the "disruption of civil aviation service" caused by "cyber attack."[3]

[3] Spokane also argues that other statutes referencing cybersecurity foreclose TSA's authority, but none of these statutes specifically implicate aviation security. *See* Federal Information Security Management Act of 2002, Pub. L. No. 107-347, Tit. III, §§ 301–05, 116 Stat. 2899, 2946–61; Federal Information Security

49 U.S.C. § 44912(b)(1)(A)(ii). These overlapping statutory authorities clearly demonstrate that TSA's regulatory mandate to protect aviation security encompasses cyberattacks.

B.

Spokane next argues the Amendment is inconsistent with TSA regulations because cybersecurity plans are not listed as one of the required elements for an airport security program in 49 C.F.R. § 1542.103.

Spokane's argument fails because the regulatory requirements for an airport security program are not exclusive. Rather, an airport security program must "[i]nclude[] the applicable items listed in § 1542.103." 49 C.F.R. § 1542.101(a)(3). If there were any doubt, the term "includes" is defined in the same chapter to mean "includes but is not limited to." *Id.* § 1500.5(b)(3). By the plain meaning of the regulation, an airport security program may be required to include more than the items detailed in section 1542.103. Moreover, TSA has the authority to amend the content of an airport security program when safety and the public interest so require. *Id.* § 1542.105(c)–(d). The Amendment adds cybersecurity plans to airport security programs, which is squarely within TSA's regulatory authority.

Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat. 3073; Cybersecurity Act of 2015, Pub. L. No. 114-113, Div. N, §§ 101–407, 129 Stat. 2242, 2935–85; Cybersecurity & Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168; Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, Div. Y, §§ 101–07, 136 Stat. 49, 1038–59. These statutes reference cybersecurity but say nothing about TSA's authority to regulate aviation security and to protect against cybersecurity threats.

Spokane also argues the Amendment is inconsistent with TSA regulations because it does not relate to "criminal violence" or "aircraft piracy" and does not directly amend the content of airport security programs. *See* 49 C.F.R. §§ 1542.101(a)(1) & 1542.105. These objections were not raised by Spokane before TSA.[4] Nor is there any evidence in the record that similar objections were made by a different participant. *See Muir v. U.S. Dep't of Homeland Sec. & TSA*, 145 F.4th 1359, 1367 (D.C. Cir. 2025) (holding courts may consider an objection if the petitioner shows "where another party raised" it below). We cannot consider Spokane's objections because they were not raised in the proceeding below. 49 U.S.C. § 46110(d).

C.

Spokane next argues the Amendment exceeds TSA's emergency rulemaking authority because it was not ratified by the Transportation Security Oversight Board. Spokane emphasizes that TSA issued the amendment without notice and comment and maintains that TSA could have done so only under its emergency rulemaking authority in 49 U.S.C. § 114(*l*)(2), which requires Board ratification of emergency rules within 90 days of promulgation.

Spokane did not raise this objection before TSA, nor was it raised by any other participant. We therefore cannot consider it. 49 U.S.C. § 46110(d). During oral argument, counsel for Spokane argued that a reference in the reconsideration petition to the applicable TSA regulations was sufficient to preserve an objection regarding the "guaranteed statutory procedure."

[4] In reply, Spokane claims it preserved the direct amendment argument, but it cites only to a part of the reconsideration petition that presented entirely different arguments.

Merely gesturing at a particular regulation, however, is not enough. To preserve an objection for judicial review under section 46110(d), a participant must provide sufficient specificity to put the agency on notice of the objection.

Moreover, the facts here demonstrate the importance of exhaustion requirements for orderly administrative and judicial proceedings. Had Spokane argued that Board ratification was required, TSA could have sought ratification at the Board's April 20, 2023, meeting—which occurred after Spokane's petition for reconsideration was filed but before it was denied by TSA.

D.

Finally, Spokane argues that TSA's issuance of the Amendment was arbitrary and capricious. Agency action must be "reasonable and reasonably explained." *FCC v. Prometheus Radio Project*, 141 S. Ct. 1150, 1158 (2021). An agency action is arbitrary and capricious if the agency "entirely failed to consider an important aspect of the problem" or "offered an explanation for its decision that runs counter to the evidence before the agency." *Motor Vehicle Mfrs. Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

Spokane raises several arguments for why the Amendment was arbitrary and capricious. First, Spokane objects to TSA's requirement that airport operators submit documentation using password-protected emails. Second, Spokane argues the Amendment irrationally allows TSA to designate systems as "critical" even if they have nothing to do with cybersecurity. Third, Spokane claims that TSA's aggregation of cybersecurity information from many airports creates a target for malicious actors. Fourth, Spokane asserts that compliance with the Amendment is too costly and requires more time. Finally, Spokane argues that, because airport security programs must

now include cybersecurity plans, the Amendment deprives airport operators of the flexibility to make improvements to those plans without TSA approval.

Spokane has failed to demonstrate the Amendment was arbitrary and capricious. As a general matter, TSA detailed the present cybersecurity threats to aviation and the cost of cyberattacks to affected entities. In light of these concerns, TSA reasonably chose to require substantial and rapid improvements in airport cybersecurity through an emergency amendment. With regard to Spokane's more specific concerns, TSA explained that the option of email submission was supported by its internal data experts and complied with federal law, and that, in any event, TSA no longer requires email submission of airport cybersecurity plans. TSA also explained that its authority to designate systems as critical—even when not so identified by airport operators—is necessary to prevent gaps in airport cybersecurity. As for data security, TSA explained it has implemented various measures and controls to secure agency data and information collected from regulated entities.

Finally, the Amendment does not unreasonably interfere with the ability of airport operators to make improvements to their cybersecurity plans. By mandating that airport security programs include cybersecurity plans, the Amendment requires operators to obtain TSA approval for changes to those plans. *See* 49 C.F.R. § 1542.105(b). Spokane characterizes this loss of flexibility as unreasonable. But given the threats to aviation, TSA reasonably concluded that large airports like Spokane must address cybersecurity in their security programs—even if that decision reduces flexibility for some operators. Moreover, the loss of flexibility is not as great as Spokane claims, since airport operators need not secure TSA approval for improvements that do not conflict with their existing security

programs. TSA also indicated that, to the extent the process for securing TSA approval impedes necessary cybersecurity improvements, it would consider changes to the amendment process in the future.

Congress has conferred substantial authority upon TSA to regulate aviation security, and we decline to disturb the agency's reasonable judgments about how to best carry out its statutory mandate. *Cf. Bonacci*, 909 F.3d at 1161–62.

* * *

TSA's broad authority over civil aviation security enables it to address cybersecurity threats to U.S. airports. Spokane failed to exhaust several of its objections before TSA, and the remaining arguments we reject on the merits. The petition for review is denied.

So ordered.