In the

United States Court of Appeals

For the Seventh Circuit

Nos. 24-2109, 24-2156 & 25-2084

GRAND TRUNK CORPORATION and ILLINOIS CENTRAL RAILROAD COMPANY, doing business as CN,

Petitioners,

v.

TRANSPORTATION SECURITY ADMINISTRATION and HA NGUYEN MCNEILL, in her official capacity as Acting Administrator of the Transportation Security Administration,

Respondents.

On Petitions for Review of Orders of the
Transportation Security Administration.
Security Directives 1580/82-2022-01B, 1580/82-2022-01C
& 1580/82-2022-01D.

ARGUED JANUARY 16, 2025 — DECIDED AUGUST 21, 2025

Before SCUDDER, KIRSCH, and LEE, *Circuit Judges*.

KIRSCH, *Circuit Judge*. In response to urgent, ongoing cybersecurity threats posed by foreign adversaries, the Transportation Security Administration issued five successive security directives requiring regulated railroads to implement a

number of expensive preventive measures. When issuing the directives, TSA bypassed notice-and-comment rulemaking by invoking an emergency-procedures exemption under 49 U.S.C. § 114(*l*)(2). Petitioners Grand Trunk Corporation and Illinois Central Railroad Company—regulated freight railroad carriers—challenge the most recent directives on various grounds, arguing chiefly that the directives were required to undergo notice and comment because the ongoing threat of cyberattacks does not constitute an emergency within the meaning of § 114(*l*)(2). But we disagree and deny the petitions, especially given the serious national security concerns attendant in this case. In doing so, we rely only on information TSA expressly included in its directives and not on any of the classified material it submitted for our review.

I

In October 2022, the Transportation Security Administration issued a security directive entitled Rail Cybersecurity Mitigation Actions and Testing. The directive expired after one year, and TSA has re-issued updated directives each year since. Grand Trunk Corporation and its subsidiary, Illinois Central Railroad Company, (collectively, CN) challenge the version of the directive issued in May 2024 as well as a July 2024 correction superseding the May directive. We heard oral argument on those challenges in January 2025. Then, in May, the July 2024 directive expired, so TSA issued a renewed directive. CN filed a separate petition challenging that May 2025 directive, which we docketed as appeal number 25-2084. Because the May 2025 directive is substantively identical to the July 2024 directive, we now consolidate CN's challenge to the May 2025 directive with its challenges to the May 2024 and July 2024 directives.

Similar to those before them, the July 2024 and May 2025 directives require certain railroads and railroad carriers—specifically, higher-risk rail operations and freight railroads that are part of the Strategic Rail Corridor Network (STRACNET)—to take extensive actions to safeguard against cybersecurity attacks. Higher-risk rail operations include carriers with annual operating revenues of $900 million or more and carriers that transport "[r]ail security-sensitive materials" like explosives, poisonous gases, hazardous liquids, and radioactive materials. See 49 C.F.R. §§ 1201.1-1(a), 1580.101, 1580.3. STRACNET railroads are part of the Department of Defense Railroads and Highways for National Defense program, which ensures that the nation's rail infrastructure can transport military supplies and equipment from fort to port in the event of a conflict. The directives require these covered railroads to enact Cybersecurity Implementation Plans, which, among other things, mandate network segmentation policies, continuous cybersecurity monitoring, and timely security patches and updates to Critical Cyber Systems. The directives also require covered railroads to develop Cybersecurity Assessment Plans and submit annual updates to TSA for approval.

Though TSA has regulated by security directive over the last few years, it has also initiated informal rulemaking. In November 2024, TSA issued a notice of proposed rulemaking and sought comments on its railroad cybersecurity plan. Enhancing Surface Cyber Risk Management, 89 Fed. Reg. 88488, 88488 (proposed Nov. 7, 2024). The comment window closed in February 2025. *Id.* TSA has taken no additional steps to promulgate a final rule. In its notice of proposed rulemaking, TSA estimated that the annual cost to the freight rail industry of complying with its cyber risk management program would

be about $100 million. *Id.* at 88535. These significant costs—many of which railroads already incur to comply with the existing security directives—in large part prompted CN's lawsuit.

At the same time, serious national security concerns motivate the security directives. The country's rail network is critical to national defense and economic vitality. The military relies on it to move supplies and equipment, and industry depends on it to transport food and manufacturing materials. As TSA explains in the July 2024 and May 2025 directives, even minor disruptions in critical rail systems could lead to temporary product shortages that would endanger our national security. And prolonged disruptions in the flow of commodities could lead to widespread supply chain disruptions, with ripple effects across the economy.

The government reports that these concerns are far from theoretical—they are real, acute, and ever-present. The July 2024 and May 2025 directives assert that "ongoing cybersecurity threat[s]" necessitate the directives: "Recent and evolving intelligence emphasizes the growing sophistication of nefarious persons, organizations, and governments, highlights vulnerabilities, and intensifies the urgency of implementing the requirements of this Security Directive." Specifically, the directives cite significant threats from foreign adversaries like Russia, China, and independent cybercriminals. For example, a joint cybersecurity advisory from the United States and allies warns "that Russia's invasion of Ukraine could expose organizations both within and beyond the region to increased malicious cyber activity … [which] may occur as a response to the unprecedented economic costs imposed on Russia as well as materiel support provided by the United States and

U.S. allies and partners." U.S. Dep't of Defense, Joint Cybersecurity Advisory, AA22-110A, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (2022).[1] The joint advisory further explains that "the Russian government is exploring options for potential cyberattacks," and details "[r]ecent Russian state-sponsored cyber operations" to underscore the looming risk of another attack. It also discusses threats made by independent cybercrime groups sympathetic to the Russian government. As for China, the directives cite another joint cybersecurity advisory that warns of a state-sponsored cyber actor whose activity "affects networks across U.S. critical infrastructure sectors." Cybersec. & Infrastructure Sec. Agency, AA23-144A, Joint Cybersecurity Advisory: People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection (2023).[2]

Additionally, the July 2024 directive relies on the 2023 Office of the Director of National Intelligence's Annual Threat Assessment of the U.S. Intelligence Community.[3] This report details acute and ongoing threats from Russia, China, Iran, and North Korea. It finds that "Russia will remain a top cyber threat as it refines and employs its espionage, influence, and attack capabilities," and explains that "Russia views cyber disruptions as a foreign policy lever to shape other countries'

---

[1] https://media.defense.gov/2022/Apr/20/2002980529/-1/-1/1/joint_csa_russian_state-spon-sored_and_criminal_cyber_threats_to_critical_infrastructure_20220420.pdf_20_22_Final.pdf, archived at https://perma.cc/4BRQ-YXW9.

[2] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a, archived at https://perma.cc/L75J-3NJP.

[3] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf, archived at https://perma.cc/B94Z-2TK3.

decisions." *Id.* at 15. Similarly, the report states that "China probably currently represents the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks." *Id.* at 10. It cautions that "China almost certainly is capable of launching cyber attacks that could disrupt critical infrastructure services within the United States, including against … rail systems." *Id.*

The May 2025 directive cites the 2025 iteration of the same report, which suggests that the cybersecurity threats have only become more urgent. Off. of the Dir. of Nat'l Intel., Annual Threat Assessment of The U.S. Intelligence Community (2025).[4] The 2025 report observes that "Russia will continue to be able to deploy anti-U.S. … cyberattacks … to try to compete below the level of armed conflict and fashion opportunities to advance Russian interests," and that "Russia's advanced cyber capabilities, its repeated success compromising sensitive targets for intelligence collection, and its past attempts to pre-position access on U.S. critical infrastructure make it a persistent counterintelligence and cyber attack threat." *Id.* at 17, 19. The report further finds that "Moscow's unique strength is the practical experience it has gained integrating cyber attacks and operations with wartime military action, almost certainly amplifying its potential to focus combined impact on U.S. targets in time of conflict." *Id.* at 19. Demonstrating the concrete risk of a Russian cyberattack, the report adds, "Russia has demonstrated real-world disruptive capabilities during the past decade, including gaining

[4] https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf, archived at https://perma.cc/824Q-2ZT3.

experience in attack execution by relentlessly targeting Ukraine's networks with disruptive and destructive malware." *Id.* at 20.

Regarding China, the 2025 report maintains that China "will continue conducting wide-ranging cyber operations against U.S. targets for both espionage and strategic advantage." *Id.* at 9. And it cites recent Chinese cybersecurity attacks on American infrastructure to emphasize the continued threat: "[China]'s campaign to preposition access on critical infrastructure for attacks during crisis or conflict, tracked publicly as Volt Typhoon, and its more recently identified compromise of U.S. telecommunications infrastructure, also referred to as Salt Typhoon, demonstrates the growing breadth and depth of [China]'s capabilities to compromise U.S. infrastructure." *Id.* at 11.

Faced with these "ongoing cybersecurity threat[s]" that may strike at any moment, the directives conclude that TSA's cybersecurity requirements "continue to be necessary to protect the national security, economy, and public health and safety of the United States and its citizens from the impact of malicious cyber-intrusions affecting the nation's railroads."

In response, CN applied directly to us for review of the May 2024, July 2024, and May 2025 directives. Title 49 U.S.C. § 46110(a) permits "a person disclosing a substantial interest in an order issued by [TSA]" under 49 U.S.C. § 114(*l*) to challenge the order "in the court of appeals of the United States for the circuit in which the person … has its principal place of business." Illinois is the principal place of business for both Grand Trunk Corporation and Illinois Central Railroad Company, so they petitioned our court for direct review collectively as CN, arguing primarily that the directives must

undergo notice and comment. CN also argues that TSA was required to conduct a cost-benefit analysis before issuing the directives, that TSA lacked statutory authority to issue the directives, and that TSA's decisions to issue the directives were arbitrary and capricious. We disagree on all fronts.

II

A

As a general matter, agencies—including TSA—may only promulgate rules after giving notice and accepting public comments. 5 U.S.C. § 553; see also *Perez v. Mortg. Bankers Ass'n*, 575 U.S. 92, 95–97 (2015). But here, a provision of TSA's enabling act, 49 U.S.C. § 114(*l*)(2), provides an exception in emergencies:

> (2) Emergency procedures.—
>
> (A) In general.—
>
> Notwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis), if the Administrator determines that a regulation or security directive must be issued immediately in order to protect transportation security, the Administrator shall issue the regulation or security directive without providing notice or an opportunity for comment and without prior approval of the Secretary.
>
> (B) Review by transportation security oversight board.—
>
> Any regulation or security directive issued under this paragraph shall be subject to review by the Transportation Security Oversight Board established under

> section 115. Any regulation or security directive issued under this paragraph shall remain effective for a period not to exceed 90 days unless ratified or disapproved by the Board or rescinded by the Administrator.

Each time TSA has issued a security directive, it has invoked § 114(*l*)(2) and claimed that this section allows it to circumvent notice and comment. CN contends otherwise, arguing that the ongoing cybersecurity threats TSA cites do not constitute an emergency justifying the evasion of notice and comment. Our question is a narrow one: does the constant cybersecurity threat presented by foreign adversaries, as described in the relevant security directives, constitute an emergency within the meaning of § 114(*l*)(2)?

CN argues for a layman's conception of emergency, contending that an emergency is a definite, unforeseen exigency that requires an immediate response. Understood this way, an emergency occurs rarely, like a "fire, flood, or earthquake." *Home Bldg. & Loan Ass'n v. Blaisdell*, 290 U.S. 398, 439 (1934). So, CN says, an ongoing threat cannot be an emergency.

CN's position has intuitive appeal. But to define emergency, we must start not with intuition but with the specific text of the statute before us. Under § 114(*l*)(2), "[e]mergency procedures" are necessary, such that TSA "shall" skip notice and comment, when TSA "determines" that "immediate[]" action is required "to protect transportation security." This standard defines the agency's emergency authority and, in broad terms, imbues TSA with significant discretion to institute procedures to mitigate sophisticated and acute cybersecurity risks facing certain rail operations and freight railroads.

Historical practice demonstrates that emergencies can be ongoing and need not be limited to a definable time period. For decades, in varied contexts, and under analogous statutes, the federal government has declared emergencies that have lasted years. For a recent example, take the COVID-19 emergency, which lasted three years. National Emergencies Act, Pub. L. No. 118-3, 137 Stat. 6 (2023) (declared under the National Emergencies Act, 50 U.S.C. §§ 1601–1651). Stretching back further, the Declaration of National Emergency by Reason of Certain Terrorist Attacks has been in effect since September 2001. Proclamation 7463, 66 Fed. Reg. 48199 (Sept. 14, 2001) (declared under National Emergencies Act); Continuation of the National Emergency With Respect to Certain Terrorist Attacks, 89 Fed. Reg. 74101 (Sept. 9, 2024). Further still, there are currently six national emergencies that have existed for over 25 years. Brennan Center for Justice, Declared National Emergencies Under the National Emergencies Act (2025).[5] That includes an emergency declared against Iran in 1979 under the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. §§ 1701–1707. See Continuation of the National Emergency With Respect to Iran, 89 Fed. Reg. 87761 (Nov. 1, 2024). Relatedly, in 1995, the President declared a separate emergency against Iran and imposed sanctions. Prohibiting Certain Transactions With Respect to the Development of Iranian Petroleum Resources, Executive Order 12957, 60 Fed. Reg. 14615 (Mar. 15, 1995) (declared under IEEPA and National Emergencies Act). That emergency is renewed annually, e.g., Continuation of the National Emergency With

---

[5] https://www.brennancenter.org/our-work/research-reports/declared-national-emergencies-under-national-emergencies-act, archived at https://perma.cc/F7JH-ZRK7.

Respect to Iran, 90 Fed. Reg. 11887 (Mar. 7, 2025), just as TSA's security directives are here. In short, long-lasting emergencies are nothing new.

And it is not as though TSA presented the cybersecurity threats as a fait accompli in October 2022 and hung its hat on the same stale intelligence ever since. Rather, TSA consults "[r]ecent and evolving intelligence" to update and revise each successive security directive. It is appropriate for TSA to rely on updated intelligence to protect transportation security by taking measures to prevent an attack. Just the same, it is also appropriate for TSA to recognize that security directives are probably not the appropriate mechanism to permanently institute elaborate compliance programs. To that end, in each revised directive, TSA has stated its "inten[t] to more permanently codify the[] [directive's] requirements through rulemaking." The recently closed comment window suggests such codification is near.

In the meantime, TSA's tailoring of the security directives to current intelligence has apparently satisfied other executive branch agencies. Under § 114(*l*)(2)(B), security directives expire after 90 days, but they may last up to a year if the Transportation Security Oversight Board ratifies them, see FAA Extension, Safety, and Security Act of 2016, Pub. L. No. 114-190, § 3409, 130 Stat. 615, 662 (2016) (TSA shall "review" and "update" security directives "annually"). The Board—comprised of representatives from the Departments of Homeland Security, Transportation, Justice, Defense, and Treasury, the Office of the Director of National Intelligence, and the National Security Council, 49 U.S.C. § 115(b)—has repeatedly

ratified the directives, indicating a unified view within the executive that the directives are necessary.[6]

We are sensitive to the longstanding tradition of affording the executive deference in matters of national security. See, e.g., *Haig v. Agee*, 453 U.S. 280, 291–92 (1981); *Trump v. Hawaii*, 585 U.S. 667, 684–87, 703–05 (2018). "[C]ourts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs" unless "Congress specifically has provided otherwise." *Dep't of Navy v. Egan*, 484 U.S. 518, 530 (1988). Here, of course, Congress has not provided otherwise; to the contrary, § 114(*l*)(2) expressly confers authority on TSA to institute emergency procedures to protect transportation security. TSA is well-equipped to do so as part of the executive branch, given the executive's intelligence capacity and ability to react promptly to risks to the nation's security. See *United States v. Curtiss-Wright Exp. Corp.*, 299 U.S. 304, 320 (1936).

Though we are mindful that "[n]ational-security concerns must not become a talisman used to ward off inconvenient claims," *Ziglar v. Abbasi*, 582 U.S. 120, 143 (2017), or to compel "abdication of the judicial role," *Holder v. Humanitarian L. Project*, 561 U.S. 1, 34 (2010), we are also loathe to "second-guess expert agency judgments on potential risks to national

[6] The May 2025 directive's 90-day expiration date was August 1, 2025. The public record does not reflect Board ratification of the May 2025 directive, but because the parties have not advised us otherwise, we presume such ratification has occurred. Previously, there have been delays between ratification and publication in the Federal Register, e.g., Ratification of Security Directives, 90 Fed. Reg. 6777-01, 6777 (Jan. 21, 2025) (publishing official notice of ratification that occurred six months earlier on July 29, 2024), and we assume the same has happened here.

security" when we traditionally "defer to the informed judgment of agency officials whose obligation it is to assess such risks," *Bonacci v. TSA*, 909 F.3d 1155, 1161–62 (D.C. Cir. 2018) (cleaned up). Congress made TSA "responsible for security in all modes of transportation," 49 U.S.C. § 114(d), and "we accord substantial deference to TSA's judgments in carrying out its statutory mandate," *Bonacci*, 909 F.3d at 1161. Typically, then, "in cases of this sort, we must defer to TSA actions that reasonably interpret and enforce the safety and security obligations of the agency." *Olivares v. TSA*, 819 F.3d 454, 462 (D.C. Cir. 2016). We see no reason to break with tradition here. We have no cause to distrust the government's intelligence reports regarding cybersecurity threats from foreign adversaries. And the applicable statute, 49 U.S.C. § 114(*l*)(2), grants TSA great latitude to determine whether those constantly looming threats—which it warns could cripple our national rail infrastructure—are an acute and ever-present problem tantamount to an ongoing emergency.

Informed by recent and evolving intelligence, TSA has exercised its discretion to determine that the threats constitute an emergency and that "security directive[s] must be issued immediately in order to protect transportation security." *Id.* Seven high-ranking officials from other agencies agreed. Given the broad statutory language empowering TSA with significant discretion, the historical precedent under analogous statutes that emergencies may last many years, the tradition of national security deference (especially to TSA on matters of transportation security), and the Transportation Security Oversight Board's ratifications, we accept TSA's determination that immediate action was required and notice and comment was not.

B

CN next argues that we must vacate the security directives because TSA failed to conduct a cost-benefit analysis. Title 49 U.S.C. § 114(*l*)(3) provides:

> In determining whether to issue, rescind, or revise a regulation under this section, the [TSA] Administrator shall consider, as a factor in the final determination, whether the costs of the regulation are excessive in relation to the enhancement of security the regulation will provide.

From this language, CN derives a requirement that TSA must conduct a cost-benefit analysis before issuing security directives. But, by its terms, § 114(*l*)(3) does not apply to security directives. Section 114(*l*)(2) references "a regulation or security directive," while § 114(*l*)(3) references only a "regulation." "Where Congress includes particular language in one section of a statute but omits it in another section of the same Act, it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion." *City & County of San Francisco v. EPA*, 145 S. Ct. 704, 713–14 (2025) (cleaned up). As such, § 114(*l*)(3) does not require TSA to consider whether the costs of a security directive are excessive in relation to the enhancement of security it will provide.

C

To issue the security directives, TSA invoked its authority under 49 U.S.C. §§ 114(d), (f), (*l*), and (m). CN argues that TSA has no substantive authority under § 114 to issue the security directives and, further, that Congress did not empower TSA to regulate rail cybersecurity at all. But CN reads § 114 too narrowly.

Congress charged TSA with "responsib[ility] for security in all modes of transportation." *Id.* § 114(d). That includes "security responsibilities over other modes of transportation that are exercised by the Department of Transportation," *id.* § 114(d)(2), which, in turn, covers railroads, see *id.* § 103. Further, Congress required that TSA "shall" "assess threats to transportation" and "develop policies, strategies, and plans for dealing with threats to transportation security." *Id.* § 114(f)(2) & (3). TSA must also "inspect, maintain, and test security facilities, equipment, and systems," "ensure the adequacy of security measures for the transportation of cargo," "oversee the implementation, and ensure the adequacy, of security measures at … transportation facilities," and "carry out such other duties, and exercise such other powers, relating to transportation security as the [TSA] Administrator considers appropriate, to the extent authorized by law." *Id.* § 114(f)(9)–(11), (16). TSA thus has extensive authority to regulate security generally for all modes of transportation, and it has authority to impose the rail cybersecurity regulations at issue here.

CN contends that § 114 only requires TSA to take actions itself and does not empower it to externally regulate the rail industry. But the statutory text is plainly to the contrary. TSA "is authorized to issue, rescind, and revise such regulations as are necessary to carry out the functions of the Administration." *Id.* § 114(*l*)(1). Because those functions include developing policies, strategies, and plans to address transportation security threats as well as assessing such threats, *id.* § 114(f)(2) & (3), TSA has the authority to issue and revise the security directives—which reflect TSA's assessment of and plans to address rail security threats. In addition, TSA's functions include affirmative obligations to regulate externally. TSA is

responsible for the security of the rail system, see *id.* § 114(d), which it protects in part by ensuring the adequacy of security measures for cargo transportation and overseeing the implementation of security measures at transportation facilities, *id.* § 114(f)(10)–(11). In sum, TSA derives power to issue the directives from a mosaic of affirmative grants of authority spread across § 114.

D

Last, CN contends that the July 2024 and May 2025 security directives were arbitrary and capricious—first, because the directives were not sufficiently tailored to the cybersecurity threats and, second, because TSA did not engage in reasoned decision-making by failing to explain why it skipped notice and comment and a cost-benefit analysis. The Administrative Procedure Act requires us to "set aside agency action" that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). To survive an arbitrary and capricious challenge, TSA's actions must "be reasonable and reasonably explained." *FCC v. Prometheus Radio Project*, 592 U.S. 414, 423 (2021).

We have already demonstrated why CN's arguments fail. First, TSA has broad authority to identify cybersecurity threats and craft appropriate responses. That's exactly what it did here, iteratively adjusting the security directives in response to recent and evolving intelligence. Further, the directives do not regulate the entire rail industry but apply narrowly only to those railroads most critical to national and economic security—higher-risk and STRACNET railroads. Second, TSA did not need to explain why it bypassed notice and comment and a cost-benefit analysis because it was not

required to undertake either measure in the first place. Accordingly, the security directives were not arbitrary or capricious.

DENIED