

**[ORAL ARGUMENT January 16, 2025]
Nos. 24-2109 (lead) & 24-2156**

**IN THE UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT**

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

Petitioners,

v.

TRANSPORTATION SECURITY ADMINISTRATION and DAVID P.
PEKOSKE, in his official capacity as Administrator of the
Transportation Security Administration,

Respondents.

On Petition for Review of an
Order of the Transportation Security Administration

OPENING BRIEF FOR PETITIONERS

Megan L. Brown
Jeremy J. Broggi
Jacqueline F. Brown
Michael J. Showalter
WILEY REIN LLP
2050 M Street NW
Washington, DC 20036
Phone: (202) 719-7000
mbrown@wiley.law
jbroggi@wiley.law
jfbrown@wiley.law
mshowalter@wiley.law

November 27, 2024

Counsel for Petitioners

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 24-2109, 24-2156

Short Caption: Grand Trunk Corp., et al. v. Transportation Security Administration, et al.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):
Grand Trunk Corporation, Illinois Central Railroad Company

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:
Wiley Rein LLP

(3) If the party, amicus or intervenor is a corporation:

i) Identify all its parent corporations, if any; and

See attached ("Responses to Question 3").

ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:

See attached ("Responses to Question 3").

(4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:

N/A

(5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:

N/A

Attorney's Signature: /s/ Megan L. Brown Date: 12-2-2024

Attorney's Printed Name: Megan L. Brown

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). Yes No

Address: 2050 M Street NW

Washington, DC 20036

Phone Number: 202.719.7579

Fax Number: 202.719.7049

E-Mail Address: MBrown@wiley.law

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 24-2109, 24-2156Short Caption: Grand Trunk Corp., et al. v. Transportation Security Administration, et al.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):
Grand Trunk Corporation, Illinois Central Railroad Company

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:
Wiley Rein LLP

(3) If the party, amicus or intervenor is a corporation:

i) Identify all its parent corporations, if any; and

See attached ("Responses to Question 3").

ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:

See attached ("Responses to Question 3").

(4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:

N/A

(5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:

N/A

Attorney's Signature: /s/ Jeremy J. Broggi Date: 11-27-2024

Attorney's Printed Name: Jeremy J. Broggi

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). Yes No

Address: 2050 M Street NW

Washington, DC 20036

Phone Number: 202.719.3747

Fax Number: 202.719.7049

E-Mail Address: JBroggi@wiley.law

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 24-2109, 24-2156

Short Caption: Grand Trunk Corp., et al. v. Transportation Security Administration, et al.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

(1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):
Grand Trunk Corporation, Illinois Central Railroad Company

(2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:
Wiley Rein LLP

(3) If the party, amicus or intervenor is a corporation:

i) Identify all its parent corporations, if any; and

See attached ("Responses to Question 3").

ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:

See attached ("Responses to Question 3").

(4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:

N/A

(5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:

N/A

Attorney's Signature: /s/ Jacqueline F. Brown Date: 12-2-2024

Attorney's Printed Name: Jacqueline F. Brown

Please indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). Yes No

Address: 2050 M Street NW

Washington, DC 20036

Phone Number: 202.719.4114

Fax Number: 202.719.7049

E-Mail Address: JFBrown@wiley.law

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 24-2109, 24-2156Short Caption: Grand Trunk Corp., et al. v. Transportation Security Administration, et al.

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

- (1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):
Grand Trunk Corporation, Illinois Central Railroad Company
- (2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:
Wiley Rein LLP
- (3) If the party, amicus or intervenor is a corporation:
- i) Identify all its parent corporations, if any; and
See attached ("Responses to Question 3").
- ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:
See attached ("Responses to Question 3").
- (4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:
N/A
- (5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:
N/A

Attorney's Signature: /s/ Michael J. Showalter Date: 12-2-2024Attorney's Printed Name: Michael J. ShowalterPlease indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d). Yes No Address: 2050 M Street NWWashington, DC 20036Phone Number: 202.719.7393Fax Number: 202.719.7049E-Mail Address: MShowalter@wiley.law

RESPONSES TO QUESTION 3

Grand Trunk Corporation is a Delaware corporation headquartered in Illinois. Its U.S. railroad operating subsidiaries are Illinois Central Railroad Company; Wisconsin Central Ltd.; Grand Trunk Western Railroad Company; Bessemer and Lake Erie Railroad Company; Chicago, Central & Pacific Company; Cedar River Railroad Company; and The Pittsburgh & Conneaut Dock Company. These subsidiaries report to the Surface Transportation Board on a consolidated Class I basis under the Grand Trunk Corporation name.

Grand Trunk Corporation is wholly owned by North American Railways, Inc.; and North American Railways, Inc. is wholly owned by Canadian National Railway Company, a publicly-owned company traded on the New York Stock Exchange (NYSE: CNI) and Toronto Stock Exchange (TSX: CNR).

Illinois Central Railroad Company is an Illinois corporation and a wholly owned indirect subsidiary of Grand Trunk Corporation.

TABLE OF CONTENTS

CIRCUIT RULE 26.1 DISCLOSURE STATEMENT	i
TABLE OF AUTHORITIES	ix
GLOSSARY	xvii
JURISDICTIONAL STATEMENT	1
INTRODUCTION	3
STATEMENT OF THE ISSUES	8
STATEMENT OF THE CASE	8
I. Congress Establishes TSA And Provides It With Targeted Authorities That Focus On Physical Aviation Security	8
II. Congress Establishes TSA’s Rulemaking Authority As Subject To Important Statutory Constraints.....	11
III. CN Commits To Freight Rail Cybersecurity At The Dawn Of The Internet Age And Maintains Robust Collaboration With Industry And Government	14
IV. TSA Unilaterally Establishes A Complex Cybersecurity Regulatory Program, Sparking Concern From Congress And Industry	18
V. TSA Extends Its Cybersecurity Regulatory Program To Freight Rail, Overlooking Congressional And Industry Concerns	21
VI. TSA Continually Expands The Scope Of Its Cybersecurity Regulatory Program And Repeatedly Renews It.....	23
VII. TSA Issues The July 2024 Security Directive, Again Expanding Its Costly Cybersecurity Program Without Public Participation	27

VIII. CN Files This Challenge To The July 2024 Security Directive..... 33

SUMMARY OF ARGUMENT..... 34

STANDARD OF REVIEW..... 37

ARGUMENT..... 38

I. The July 2024 Security Directive Violates Section 114(l)'s Notice And Comment Rulemaking Requirement 38

A. Section 114 Requires Rulemaking Absent An Emergency 38

B. The July 2024 Security Directive Relies On A Threat, Not An Emergency 42

C. A Threat Is Not An Emergency 45

D. The July 2024 Security Directive Establishes A Highly Prescriptive And Indefinite Regulatory Program That Demands Rulemaking..... 51

E. Vacatur Is Required..... 54

II. The July 2024 Security Directive Violates Section 114(l)'s Directive To Consider Costs And Benefits..... 55

III. The July 2024 Security Directive Fails To Identify Any Grant Of Substantive Regulatory Authority Over Cybersecurity 58

A. Substantive Rulemaking Requires Substantive Authority 59

B. Section 114 Does Not Grant TSA Substantive Authority To Impose The Security Directive 60

IV. The July 2024 Security Directive Is Not Tailored To The Purported Threats And Is Otherwise Arbitrary 65

CONCLUSION69

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>A.L.A. Schechter Poultry Corp. v. United States</i> , 295 U.S. 495 (1935)	63
<i>Ala. Ass’n of Realtors v. HHS</i> , 594 U.S. 758 (2021)	50, 59, 60
<i>Alaska Airlines, Inc. v. TSA</i> , 588 F.3d 1116 (D.C. Cir. 2009)	9
<i>Am. Forest & Paper Ass’n v. EPA</i> , 137 F.3d 291 (5th Cir. 1998)	65
<i>Azar v. Allina Health Servs.</i> , 587 U.S. 566 (2019)	52
<i>Batterton v. Marshall</i> , 648 F.2d 694 (D.C. Cir. 1980)	52
<i>Bd. of Educ. of Ottawa Twp. High Sch. Dist. 140 v. Spellings</i> , 517 F.3d 922 (7th Cir. 2008)	2
<i>Biden v. Nebraska</i> , 143 S. Ct. 2355 (2023)	51
<i>Boucher v. USDA</i> , 934 F.3d 530 (7th Cir. 2019)	68, 69
<i>BST Holdings, LLC v. OSHA</i> , 17 F.4th 604 (5th Cir. 2021)	48
<i>Carpenters Indus. Council v. Zinke</i> , 854 F.3d 1 (D.C. Cir. 2017)	2
<i>Cent. Forwarding, Inc. v. ICC</i> , 698 F.2d 1266 (5th Cir. 1983)	50

Chamber of Com. of U.S. v. SEC,
88 F.4th 1115 (5th Cir. 2023) 55, 58

Cisneros v. Alpine Ridge Grp.,
508 U.S. 10 (1993)..... 56

Citizens Ins. Co. of Am. v. Wynndalco Enters., LLC, 70 F.4th 987 (7th Cir. 2023)..... 39

Corner Post, Inc. v. Bd. of Governors of Fed. Rsrv. Sys.,
144 S. Ct. 2440 (2024)..... 54

Dep’t of Com. v. New York,
588 U.S. 752 (2019) 42, 66

DHS v. MacLean,
574 U.S. 383 (2015)..... 62

DirectTV, Inc. v. Barczewski,
604 F.3d 1004 (7th Cir. 2010)..... 39

Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council,
485 U.S. 568 (1988)..... 64

FCC v. Prometheus Radio Project,
592 U.S. 414 (2021) 38

FEC v. Cruz,
596 U.S. 289 (2022) 59

Five Points Rd. Joint Venture v. Johanns,
542 F.3d 1121 (7th Cir. 2008)..... 12

Grand Trunk Corp. v. TSA,
No. 24-2109 (7th Cir. filed June 28, 2024)..... 27, 28, 29

Grand Trunk Corp. v. TSA,
No. 24-2156 (7th Cir. filed July 8, 2024)..... 33

Groff v. DeJoy,
600 U.S. 447 (2023) 38

Gundy v. United States,
588 U.S. 128 (2019) 63

Home Bldg. & Loan Ass’n v. Blaisdell,
290 U.S. 398 (1934) 46, 47

Ill. Citizens Comm. for Broad. v. FCC,
467 F.2d 1397 (7th Cir. 1972) 60

Ill. State Chamber of Com. v. EPA,
775 F.2d 1141 (7th Cir. 1985) 55

Illinois v. United States,
666 F.2d 1066 (7th Cir. 1981) 58

Interstate Nat. Gas Ass’n of Am. v. PHMSA,
114 F.4th 744 (D.C. Cir. 2024) 58

Johnson v. OPM,
783 F.3d 655 (7th Cir. 2015) 55

Loper Bright Enters. v. Raimondo,
144 S. Ct. 2244 (2024) 37, 38

Lujan v. Defs. of Wildlife,
504 U.S. 555 (1992) 2

Merck & Co. v. HHS,
385 F. Supp. 3d 81 (D.D.C. 2019), *aff’d*, 962 F.3d 531 (D.C.
Cir. 2020) 59

Michigan v. EPA,
576 U.S. 743 (2015) 57

*Motor Vehicle Mfrs. Ass’n of U.S. v. State Farm Mut. Auto.
Ins. Co.*,
463 U.S. 29 (1983) 66, 69

Nat. Res. Def. Council v. Wheeler,
955 F.3d 68 (D.C. Cir. 2020) 54

Neustar, Inc. v. FCC,
857 F.3d 886 (D.C. Cir. 2017) 64

New York Stock Exch. LLC v. SEC,
962 F.3d 541 (D.C. Cir. 2020) 59

NFIB v. OSHA,
595 U.S. 109 (2022) 48, 51, 59

Niz-Chavez v. Garland,
593 U.S. 155 (2021) 3

Nw. Tissue Ctr. v. Shalala,
1 F.3d 522 (7th Cir. 1993) 52

Pan. Refin. Co. v. Ryan,
293 U.S. 388 (1935) 64

Pension Benefit Guar. Corp. v. LTV Corp.,
496 U.S. 633 (1990) 42

Platte River Whooping Crane Tr. v. FERC,
962 F.2d 27 (D.C. Cir. 1992) 65

Sorenson Commc’ns Inc. v. FCC,
755 F.3d 702 (D.C. Cir. 2014) 45

Town of Barnstable, Mass. v. FAA,
659 F.3d 28 (D.C. Cir. 2011) 55

United States v. Davis,
29 F.4th 380 (7th Cir. 2022) 64

Wayman v. Southard,
23 U.S. (10 Wheat) 1 (1825) 63

Statutes

5 U.S.C. § 553 52

5 U.S.C. § 702 1

5 U.S.C. § 706 37

16 U.S.C. § 824..... 49

29 U.S.C. § 655..... 47

49 U.S.C. § 114..... 9, 11, 12, 31, 32, 35, 38, 39, 40, 61

49 U.S.C. § 115..... 22

49 U.S.C. § 44901..... 10

49 U.S.C. § 44902..... 14

49 U.S.C. § 44903..... 10, 14

49 U.S.C. § 44917..... 9

49 U.S.C. § 44921..... 9

49 U.S.C. § 46110..... 1, 37, 55

49 U.S.C. § 48301..... 9

Aviation and Transportation Security Act, Pub. L. 107–71,
115 Stat. 597 (2001) 9

Regulatory Materials

49 C.F.R. § 1580.1 28

Air Cargo Screening, Interim Final Rule, 74 Fed. Reg. 47672
(Sept. 16, 2009)..... 13

Consolidated Reporting by Commonly Controlled Railroads,
5 S.T.B. 1050 (2001), *codified at* 49 C.F.R. § 1201(1-
1)(b)(1) 1

Criteria for Preparation and Evaluation of Radiological
Emergency Response Plans and Preparedness in Support
of Nuclear Power Plants, Notification of Availability, 84
Fed. Reg. 70435 (Dec. 23, 2019) 53

Enhancing Surface Cyber Risk Management, Advance
 Notice of Proposed Rulemaking, 87 Fed. Reg. 73527 (Nov.
 30, 2022) 25, 26

Enhancing Surface Cyber Risk Management, Notice of
 Proposed Rulemaking, 89 Fed. Reg. 88488 (Nov. 7, 2024) 32, 33

Improving Regulation and Regulatory Review, 76 Fed. Reg.
 3821 (Jan. 18, 2011) (Executive Order 13563) 57

Incentives for Advanced Cybersecurity Investment, Final
 Rule, 88 Fed. Reg. 28348 (May 3, 2023)..... 53

Medications for the Treatment of Opioid Use Disorder, Final
 Rule, 89 Fed. Reg. 7528 (Feb. 2, 2024)..... 53

Passenger Screening Using Advanced Imaging Technology,
 Final Rule, 81 Fed. Reg. 11364 (Mar. 3, 2016) 13, 53

Ratification of Security Directives, 87 Fed. Reg. 31093 (May
 23, 2022) 22, 43

Ratification of Security Directives, 88 Fed. Reg. 36921 (June
 6, 2023) 43

Ratification of Security Directives, 89 Fed. Reg. 28570 (Apr.
 19, 2024) 18

Security Training for Surface Transportation Employees,
 Final Rule, 85 Fed. Reg. 16456 (Mar. 23, 2020) 14

Other Authorities

Antonin Scalia & Brian A. Garner, *Reading Law: The
 Interpretation of Legal Texts* (2012) 39

The American Heritage Dictionary of the English Language
 (4th ed. 2000)..... 46

Amy L. Stein, *Energy Emergencies*, 115 Nw. U. L. Rev. 799
 (2020) 49

Association of American Railroads, *Railroads and Cybersecurity*, (March 2018), tinyurl.com/45df83z9..... 15

Black’s Law Dictionary (7th ed. 1999)..... 47

Black’s Law Dictionary (11th ed. 2019)..... 39

Black’s Law Dictionary (12th ed. 2024)..... 46

Cambridge Dictionary of American English (Sidney I. Landau 2000) 46, 47

CN, *2023 Annual Report* (2024), tinyurl.com/3cpyuxzk 16

CN, *About CN*, tinyurl.com/65756tht 15

CN, “Risk and Business Continuity Management,” tinyurl.com/34sxum57 (last visited Nov. 24, 2024) 16

Cong. Rsch. Serv., 98-505, National Emergency Powers (2021)..... 46, 54

DHS, *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators* (May 27, 2021) 18

DHS, *Secretary Mayorkas Delivers Remarks at the 12th Annual Billington CyberSecurity Summit* (Oct. 6, 2021)..... 18, 19

Elena Chachko & Katerina Linos, *Emergency Powers for Good*, 66 William & Mary L. Rev., available at <https://tinyurl.com/mu754bn7> 49

Impacts of Emergency Authority Cybersecurity Regulations on the Transportation Sector: Hearing Before the Committee on Homeland Security, 118th Cong. (Nov. 19, 2024), available at tinyurl.com/dppduhgy 20

Jonathan Greig, *TSA to change cybersecurity rules for pipelines following industry criticism*, The Record (June 28, 2022), tinyurl.com/4xhzbtjr 22, 23, 45

Max Skonsberg, *Burke, A Man for All Seasons*, Law & Liberty (Aug. 5, 2024), tinyurl.com/47vhdrdw 49

Memo re Face Mask Requirements Security Directive 1544-21-02 (Jan. 31, 2021), tinyurl.com/2zufy7j3 14

The New Oxford American Dictionary (Elizabeth J. Jewell & Frank Abate 2001) 47

Office of the Director of National Intelligence, *Annual Threat Assessment of The U.S. Intelligence Community* (Feb. 6, 2023) 17

Random House Webster’s College Dictionary (2000)..... 47

TSA Supp. Br., *Wall v. TSA*, No. 21-1220, 2023 WL 1830810 (D.C. Cir. Feb. 9, 2023) 4, 41

TSA, Transportation Security Timeline, *TSA Issues New Cybersecurity Requirements for Airport and Aircraft Operators* (last visited Nov. 24, 2024)..... 44

GLOSSARY

APA	Administrative Procedure Act
CDC	Centers for Disease Control and Prevention
DHS	Department of Homeland Security
FERC	Federal Energy Regulatory Commission
OSHA	Occupational Safety and Health Administration
TSA	Transportation Security Administration

JURISDICTIONAL STATEMENT

This Court has appellate jurisdiction to review the challenged Security Directive because it is “an order issued by ... the Administrator of the Transportation Security Administration ... in whole or in part under ... subsection (l) ... of section 114.” 49 U.S.C. § 46110(a); *see* 5 U.S.C. § 702. The Petition is timely because the Security Directive was issued July 1, 2024, and the Petition was filed on July 8, 2024—*i.e.*, “not later than 60 days after the order [was] issued.” 49 U.S.C. § 46110(a).

Venue lies in this Court because Petitioner Grand Trunk Corporation, a Delaware corporation, and Petitioner Illinois Central Railroad Company, an Illinois corporation (itself an operating rail subsidiary of Grand Trunk Corporation), each has its principal place of business in Illinois. *See id.* The companies report to the Surface Transportation Board on a consolidated Class I basis under the name of Grand Trunk Corporation, *see* Consolidated Reporting by Commonly Controlled Railroads, 5 S.T.B. 1050 (2001), *codified at* 49 C.F.R. § 1201(1-1)(b)(1), and do business under the name “CN.”

Petitioners have Article III standing because the Security Directive directly regulates Class I freight railroads, including Petitioners. *See*

Lujan v. Defs. of Wildlife, 504 U.S. 555, 561–62 (1992) (“w[hen] the plaintiff is himself an object of the action ... there is ordinarily little question that the action ... has caused him injury, and that a judgment preventing ... the action will redress it”). Class I freight railroads including Petitioners must expend significant financial resources to comply with TSA’s directives. App.141 (TSA, Meeting Minutes re TSA Policy Position on Positive Train Control (PTC) Systems as Critical Cyber Systems, at 4 (Aug. 23, 2023)) (“Meeting Minutes”) (estimating “a \$100-million-dollar difference”); App.145–46 (Association of American Rail, White Paper on Status of Positive Train Control and TSA SD 1580/82-2022-01 (Sept. 22, 2023)) (“Association of American Railroads White Paper”) (estimating costs in “hundreds of millions of dollars”). That is injury-in-fact. *See, e.g., Bd. of Educ. of Ottawa Twp. High Sch. Dist. 140 v. Spellings*, 517 F.3d 922, 925 (7th Cir. 2008) (plaintiffs had standing where “[c]ompliance with [a regulation] [was] expensive”); *Carpenters Indus. Council v. Zinke*, 854 F.3d 1, 5 (D.C. Cir. 2017) (Kavanaugh, J.) (“Economic harm to a business clearly constitutes an injury-in-fact.”). Because Petitioners’ injury is caused by the challenged Security

Directive, it would be redressed by an order setting the Security Directive aside.

INTRODUCTION

The Transportation Security Administration must “turn square corners” when it regulates Americans. *Niz-Chavez v. Garland*, 593 U.S. 155, 172 (2021). But when imposing new cybersecurity mandates on freight rail companies beginning in June 2021 and culminating in a July 2024 Security Directive that currently regulates industry, TSA flagrantly violated federal statutory law by skipping a required step. CN has been committed to cybersecurity since the internet age began and holds a sterling record of defeating cyber threats. CN supports industry adoption of cybersecurity best practices and has adopted those practices itself. But CN does not support agency action that does not comply with plain statutory text.

The Aviation and Transportation Security Act, enacted in November 2001 in the aftermath of September 11, created TSA and gave it circumscribed substantive regulatory authority. On procedure, the Act requires notice and comment “in general” and authorizes TSA to bypass notice and comment only when a security directive “must be issued

immediately” because of an “[e]mergency.” But TSA concedes that it did not provide notice and comment for its freight rail cybersecurity mandates—it simply announced them with private letters to industry. And while TSA invoked its power to bypass notice and comment in emergencies, TSA did not cite any emergency nor claim that there are exigent circumstances. In explaining its motivation, remarkably, the July 2024 Security Directive never even uses the word “emergency.”

Instead, the Government has unironically asserted that TSA may use its emergency power routinely. TSA, the Government has explained, “regularly” “issues security directives without notice and comment.” TSA Supp. Br. 9, *Wall v. TSA*, No. 21-1220, 2023 WL 1830810 (D.C. Cir. Feb. 9, 2023) (TSA brief available at 2022 WL 4182503). According to the Government, security directives “generally” do not require notice and comment. *Id.* at 7. That claim is certainly consistent with TSA’s behavior here, where it has used security directives to impose and then iterate a complex regulatory scheme for several years, without ever appropriately taking input from regulated industry or the public. But it stands 180 degrees from the statutory text and scheme, which “in general” requires notice and comment.

Here, TSA candidly acknowledged that its July 2024 Security Directive is designed prophylactically to head off some unknown future cybersecurity incident. In other words, the Security Directive addresses the “threat” of cybercrime, which is “persistent” and “ever-present,” as TSA put it repeatedly. TSA cited nothing that conceivably could even be conceptualized as an acute impending crisis. And chronic threat is not emergency. Members of this world will always face the threat of cybercrime, among many others. Calling our condition a perpetual “emergency” would divest that word of its meaning, and would permanently endow government with all kinds of extraordinary powers that are supposed to be reserved for extraordinary times. If threat equals emergency, then TSA *never* need provide notice and comment—and other federal agencies will have perpetual access to their emergency powers too. That dangerous proposition is not the law.

The amount of time passed since TSA first imposed its cybersecurity mandates underscores the absence of any true emergency. An “emergency,” the Congressional Research Service has explained, is something so unforeseen, infrequent, and unstable that it does not “admit of ... being dealt with according to rule.” The very reason the Act makes

an exception for emergencies is that notice and comment could take too long to address an exigency. But TSA's cybersecurity mandates have been in force for more than three years. TSA has identified no reason it could not have promulgated its cybersecurity mandates "according to rule" in July 2021. Indeed, that first security directive expired after a year, but TSA has maintained its cybersecurity mandates by reissuing the "same" security directive (TSA's word) every year. (In fact TSA has incrementally added burdens on industry with each successive security directive.) The Act does not allow circumvention of its notice-and-comment requirement under these circumstances.

TSA committed a second error, furthermore, by failing to conduct a statutorily required cost/benefit analysis. The Act provides that when issuing a regulation "under [the] section" TSA invoked in the July 2024 Security Directive, TSA must consider "whether the costs of the regulation are excessive in relation to the enhancement of security the regulation will provide." TSA has conceded that it did not consider the July 2024 Security Directive's costs relative to its purported enhancement of security, and the July 2024 Security Directive must be vacated for that reason independently.

On substance, TSA's cybersecurity mandates are unlawful because TSA has not cited any provision of the Act granting TSA the substantive authority to regulate industry with the hypertechnical cybersecurity requirements the July 2024 Security Directive imposes. Indeed, the July 2024 Security Directive does not cite any substantive authority that authorizes TSA to regulate freight rail cybersecurity at all.

The July 2024 Security Directive also is arbitrary and capricious because the granular requirements it imposes are not tailored to the purported threats it identifies. For example, the July 2024 Security Directive cites the threat of spam and phishing emails, but then reaches far beyond those issues by micromanaging railroad internal cybersecurity practices. And TSA acted arbitrarily and capriciously additionally by failing to offer any explanation for its decision to use emergency procedures and to forego cost/benefit analysis after industry raised those issues.

TSA's July 2024 Security Directive is clearly unlawful, and this Court should vacate it.

STATEMENT OF THE ISSUES

1) Whether the “ever-present threat” of cybercrime is an “emergency” that allows TSA to bypass notice-and-comment rulemaking under 49 U.S.C. § 114(l).

2) Whether Section 114(l)(3) required TSA to consider the July 2024 Security Directive’s costs and benefits.

3) Whether the statutory provisions TSA cited grant it substantive regulatory authority to impose the July 2024 Security Directive’s micromanaging regulatory scheme.

4) Whether TSA acted arbitrarily and capriciously by failing to tailor the July 2024 Security Directive’s requirements to the purported threats and by failing to explain its decisions to forego notice and comment and consideration of costs and benefits.

STATEMENT OF THE CASE

I. Congress Establishes TSA And Provides It With Targeted Authorities That Focus On Physical Aviation Security

On September 11, 2001, terrorists hijacked four commercial planes and murdered more than three thousand Americans. In November 2001, Congress and President Bush enacted the Aviation and Transportation Security Act. The Act is captioned: “An act to improve airport security,

and for other purposes.” Pub. L. 107–71, 115 Stat. 597 (2001) (the “Act”). The Act created TSA to oversee security for all modes of transportation, with a strong focus on aviation. *See* 49 U.S.C. § 114(d); *see also Alaska Airlines, Inc. v. TSA*, 588 F.3d 1116, 1117–18 (D.C. Cir. 2009) (the Act “establish[ed] the TSA and vest[ed] it with primary responsibility for maintaining civil air security”). TSA assumed responsibility for airport security, which was previously handled by private contractors. Congress did not create TSA to act as a general cybersecurity regulator or to reshape various modes of transportation.

The Act mandates federal employees to conduct passenger and baggage screenings at commercial airports. *See* 49 U.S.C. § 114(e). These screeners, under TSA oversight, are responsible for enforcing security measures to prevent dangerous items from being brought onto planes. The Act expanded the Federal Air Marshal Service, placing armed federal law enforcement officers aboard certain flights to enhance onboard security. *See id.* § 44917. The Act strengthened cockpit door security and allowed pilots to be armed through the Federal Flight Deck Officer program. *See id.* §§ 48301(b)(1), 44921. The Act introduced more

rigorous passenger pre-boarding screening procedures, including no-fly lists and enhanced background checks. *See id.* §§ 44901, 44903(j)(2).

The Act also specifies a series of additional TSA functions:

- (1) receive, assess, and distribute intelligence information related to transportation security;
- (2) assess threats to transportation;
- (3) develop policies, strategies, and plans for dealing with threats to transportation security;
- (4) make other plans related to transportation security, including coordinating countermeasures with appropriate departments, agencies, and instrumentalities of the United States Government;
- (5) serve as the primary liaison for transportation security to the intelligence and law enforcement communities;
- (6) on a day-to-day basis, manage and provide operational guidance to the field security resources of the Administration, including Federal Security Managers as provided by section 44933;
- (7) enforce security-related regulations and requirements;
- (8) identify and undertake research and development activities necessary to enhance transportation security;
- (9) inspect, maintain, and test security facilities, equipment, and systems;
- (10) ensure the adequacy of security measures for the transportation of cargo;
- (11) oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities;

(12) require background checks for airport security screening personnel, individuals with access to secure areas of airports, and other transportation security personnel;

(13) work in conjunction with the Administrator of the Federal Aviation Administration with respect to any actions or activities that may affect aviation safety or air carrier operations;

(14) work with the International Civil Aviation Organization and appropriate aeronautic authorities of foreign governments under section 44907 to address security concerns on passenger flights by foreign air carriers in foreign air transportation;

(15) establish and maintain a National Deployment Office ...; and

(16) carry out such other duties, and exercise such other powers, relating to transportation security as the Administrator considers appropriate, to the extent authorized by law.

Id. § 114(f).

II. Congress Establishes TSA’s Rulemaking Authority As Subject To Important Statutory Constraints

Although not designed principally as a regulatory agency, the Act grants TSA rulemaking authority in Section 114(l). That Section has three subsections pertinent here.

The first is titled “(1) In general.” It provides that TSA is authorized to promulgate regulations as necessary to carry out its functions, subject of course to the rulemaking requirements of the

Administrative Procedure Act. *See, e.g., Five Points Rd. Joint Venture v. Johanns*, 542 F.3d 1121, 1126–27 (7th Cir. 2008) (“the APA specifically states that a ‘subsequent statute may not be held to supersede or modify [the APA] ... except to the extent that it does so expressly’” (quoting 5 U.S.C. § 559)).

The second subsection is titled “(2) Emergency procedures.” It provides that if TSA “determines that a regulation or security directive must be issued immediately in order to protect transportation security,” then TSA shall issue the regulation or security directive “without providing notice or an opportunity for comment and without prior approval of the Secretary.” 49 U.S.C. § 114(l)(2)(A). And the regulation or security directive shall expire in 90 days “unless ratified or disapproved by the [Transportation Security Oversight] Board or rescinded by the Administrator.” *Id.*

The third subsection is titled “(3) Factors to consider.” It provides that in determining whether to promulgate a regulation “under this section,” TSA “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.”

Historically, TSA has recognized that notice-and-comment regulations promulgated under Subsection (l) must be premised on powers specifically enumerated in a federal statute. For example, TSA has promulgated a rule requiring advanced imaging technology screening for civil aviation passengers, citing 49 U.S.C. § 114(e), which makes TSA “responsible for day-to-day Federal security screening operations for passenger air transportation.” Passenger Screening Using Advanced Imaging Technology, Final Rule, 81 Fed. Reg. 11364, 11365, 11389 (Mar. 3, 2016). That rule also cites 49 U.S.C. § 44925, which specifically authorizes the Department of Homeland Security to develop and deploy detection equipment at airport screening checkpoints. Similarly, TSA has promulgated an air-cargo-screening rule that relies on a provision of the Implementing Recommendations of the 9/11 Commission Act of 2007 (“9/11 Act”), 49 U.S.C. § 44901(g)(1), which requires TSA to establish a system to screen passenger-aircraft cargo. Air Cargo Screening, Interim Final Rule, 74 Fed. Reg. 47672, 47674 (Sept. 16, 2009). A different TSA rule requiring security training for surface transportation employees cites other provisions of the 9/11 Act (6 U.S.C. §§ 1137, 1167, and 1184) that grant authority to promulgate regulations to enhance surface-

transportation security through security training of frontline employees. Security Training for Surface Transportation Employees, Final Rule, 85 Fed. Reg. 16456, 16457 n.6 (Mar. 23, 2020).

The same is true when TSA has issued regulations under its emergency procedures. For example, when TSA issued a security directive to “support[] enforcement” of a Centers for Disease Control and Prevention order mandating masks on aircraft, *see* Memo re Face Mask Requirements Security Directive 1544-21-02, at 1 (Jan. 31, 2021), tinyurl.com/2zufy7j3, TSA cited substantive statutory grants that authorize it to make rules to “protect passengers ... on an aircraft” and to govern when an air carrier may “refuse to transport” a passenger who does not comply with TSA safety regulations. 49 U.S.C. §§ 44902, 44903(b); *see* Face Mask Requirements Security Directive, at 1. That security directive described an emergency regarding Covid-19. Face Mask Requirements Security Directive, at 1.

III. CN Commits To Freight Rail Cybersecurity At The Dawn Of The Internet Age And Maintains Robust Collaboration With Industry And Government

CN is a public company that operates a nearly 20,000-mile freight railway spanning Canada and mid-America and connecting ports on

three coasts. CN's freight services are essential to the United States and broader North American economy, employing approximately 23,000 railroaders and transporting approximately \$178 billion worth of goods annually for a wide range of business sectors. *See* CN, *About CN*, tinyurl.com/65756tth.

For decades, CN and the freight-rail industry have pioneered railroad safety innovations and have focused on cybersecurity since before TSA existed. The industry's cybersecurity collaboration forum, the Rail Information Security Committee, was created in 1999—two years before TSA was established in 2001. *See* Association of American Railroads, *Railroads and Cybersecurity*, (March 2018), tinyurl.com/45df83z9. CN's U.S. subsidiaries—Grand Trunk Corporation and Illinois Central (the Petitioners here)—were founding members of the Committee and on the front lines of enhancing freight rail cybersecurity well before cybersecurity became an emphasis by government and other businesses.

CN maintains its robust commitment to cybersecurity today. Its cybersecurity program predates TSA's security directives and includes approximately 80 dedicated specialized technical staff members led by a

Chief Information Security Officer and overseen by the Audit Finance and Risk Committee of its Board of Directors. CN has made substantial investments in cybersecurity capabilities, information technology risk management, business continuity and disaster recovery plans, and other security and mitigation programs. CN, *2023 Annual Report*, at 63–64 (2024), tinyurl.com/3cpyuxzk. Beyond its personnel and technological capabilities, CN’s cybersecurity program is aligned with the National Institute of Standards and Technology’s Cybersecurity Framework, and includes a robust cybersecurity incident response plan, recurring vulnerability assessments, and threat intelligence sharing with industry partners and government agencies in the U.S. and Canada. CN’s cyber risk management activities also include employee training and use independent third parties for penetration testing and assessments of the cybersecurity program on at least an annual basis. *See* CN, “Risk and Business Continuity Management,” tinyurl.com/34sxum57 (last visited Nov. 24, 2024).

These substantial investments by CN and others in the freight rail industry have been a success. Despite the ever-increasing amount of malicious cyber activity targeted against U.S. Government and private-

sector networks in general, AR108 (Office of the Director of National Intelligence, *Annual Threat Assessment of The U.S. Intelligence Community*, at 10 (Feb. 6, 2023), tinyurl.com/4968xntu) (describing a “persistent cyber espionage threat to U.S. Government and private-sector networks”), freight rail cybersecurity has remained a relative bright spot in successfully mitigating such activity for *years*. According to TSA’s most recent annual Transportation Cyber Incident Executive Summary (and contrary to the agency’s position here that it “must” act “immediately” to protect freight rail), the Government’s intelligence “reporting did not reveal a notable cyber incident that caused an operational impact for a freight rail entity in 2023.” AR686 (TSA, 2023 Annual Global Transportation Cyber Incident Executive Summary, at 5).¹

¹ TSA says the 2023 Transportation Cyber Incident Executive Summary is part of the administrative record and has filed it with the Court under seal. *See* Certified Index to the Unclassified Administrative Record (Oct. 18, 2024), Dkt. 15; AR682–93. The sentence quoted above is portion marked by TSA as unclassified and subject to no dissemination restrictions. In response to a request from counsel, the Government stated its agreement that this sentence is fully unclassified and not subject to the protective order and may be included in Petitioners’ publicly filed opening brief.

IV. TSA Unilaterally Establishes A Complex Cybersecurity Regulatory Program, Sparking Concern From Congress And Industry

Not every transportation sector has had the same success as freight rail. In May 2021, a pipeline company called Colonial Pipeline suffered a major cybersecurity attack. In response, later that month, TSA issued Security Directive Pipeline-2021-01 to pipeline companies. *See* DHS, *DHS Announces New Cybersecurity Requirements for Critical Pipeline Owners and Operators* (May 27, 2021), tinyurl.com/3ynu2tsm.²

TSA did not initially design or apply its new cybersecurity regulatory program to freight rail. But in October 2021, DHS Secretary Alejandro Mayorkas discussed new cyber measures in a keynote address at a cybersecurity summit. DHS, *Secretary Mayorkas Delivers Remarks at the 12th Annual Billington CyberSecurity Summit* (Oct. 6, 2021), tinyurl.com/3cfvwe8k. Secretary Mayorkas noted that the country's

² The pipeline security directive, which has been continued with subsequent security directives, required covered pipeline companies to: (1) report cybersecurity incidents to the Cybersecurity and Infrastructure Security Agency (CISA); (2) appoint a cybersecurity coordinator to be available to coordinate with TSA and CISA; and (3) conduct a self-assessment of cybersecurity practices, identify any gaps, and develop a plan and timeline for remediation. *See* Ratification of Security Directives, 89 Fed. Reg. 28570, 28570 (Apr. 19, 2024).

freight-rail system is “essential ... to our economic well-being” and to “the ability of our military to move equipment from ‘Fort to Port’ when needed.” *Id.* He stated that “[t]o strengthen the cybersecurity of our railroads and rail transit,” TSA would “issue a new security directive this year that will cover higher-risk railroad and rail transit entities.” *Id.* He did not identify any emergency necessitating the security directive. *Id.* He opined, however, that the measures identified by the government as relevant to the pipeline sector were “important,” and suggested that in the absence of mandating them for rail, rail could “become a victim of malicious cyber activity.” *Id.* For less “important” measures, he continued, TSA would initiate “a rulemaking process to develop a longer-term regime to strengthen cybersecurity.” *Id.*

Secretary Mayorkas’ failure to identify any emergency or rail-specific concerns was consistent with contemporaneous threat reporting from TSA to the industry. In September 2021, a “senior TSA Surface official” had told industry representatives in a teleconference that “no imminent or elevated cyber threat pertains to railroads.” App.99 (TSA, Industry Comments and Questions re SDs 1580-21-01 and 1582-21-01 (Oct. 5, 2021)) (“Industry Comments and Questions”). Rather, the official

described the threat as “persistent” and asserted that it “pertains for the transportation modes generally.” *Id.*; see also *Impacts of Emergency Authority Cybersecurity Regulations on the Transportation Sector: Hearing Before the Committee on Homeland Security*, 118th Cong. (Nov. 19, 2024) (statement of Ian Jefferies, President and CEO, Association of American Railroads) (“AAR was unaware of, nor was it made aware of, any prevailing freight rail emergency conditions that would require use of emergency authority.”), *available at* tinyurl.com/dppduhgy.

In October 2021, a group of U.S. senators wrote a letter to DHS’s inspector general expressing concern about TSA’s process for issuing its security directives. App.115 (Letter from Sens. Rob Portman, James Lankford, M. Michael Rounds, to Hon. Joseph V. Cuffari, Inspector General, DHS, at 1 (Oct. 28, 2021), tinyurl.com/mp7vwact). Though “agree[ing] [with TSA] that critical infrastructure must be protected against cyber-attacks,” the Senators emphasized that “the process by which TSA has issued these directives raises concerns.” App.116 (*Id.* at 2). The “recently issued security directives,” the Senators observed, “depart from TSA’s historically collaborative relationship with industry experts.” App.115 (*Id.* at 1). Previously, TSA “had worked in close

coordination with industry stakeholders to develop practical security guidelines and policies.” App.115 (*Id.*). With additional rail and aviation security directives forthcoming, TSA “provided very little time for industry feedback.” App.116 (*Id.* at 2). And TSA invoked its emergency Section 114(*l*)(2) authority, which “had never before been exercised with the pipeline sector.” App.115 (*Id.* at 1). The Senators urged TSA to identify “the basis for employing the emergency authority under section 114(*l*)(2) ... to issue those directives without full notice and comment.” App.116 (*Id.* at 2). The agency did not do these things.

V. TSA Extends Its Cybersecurity Regulatory Program To Freight Rail, Overlooking Congressional And Industry Concerns

In December 2021, TSA for the first time issued a freight rail cybersecurity security directive, titled “Enhancing Rail Cybersecurity.” App.2 (TSA, Security Directive 1580-21-01, Enhancing Rail Cybersecurity (Dec. 31, 2021), tinyurl.com/mvct3phe).³ This security directive required all freight railroad carriers to designate a

³ On the same day, TSA issued an “identical” security directive for passenger rail, titled “Enhancing Public Transportation and Passenger Rail Cybersecurity.” App.1 (TSA, Transmittal Memo re: Issuance of SD 1580-2021-01 and SD 1582-2021-01 (Dec. 1, 2021)). That security directive is not at issue here.

Cybersecurity Coordinator, report cybersecurity incidents to CISA, develop a Cybersecurity Incident Response Plan, and conduct a cybersecurity vulnerability assessment. App.2–3 (*Id.* at 1–2).

TSA’s stated purpose was addressing the “ongoing” cybersecurity “threat” and to prevent harm that “could result” from a cyberattack. Although TSA did not claim that there was any “emergency,” the agency stated that the security directive was being issued “under the authority of 49 U.S.C. [§] 114(l)(2)(A).” App.2 (*Id.* at 1). TSA announced the security directive through private letters to regulated entities. TSA did not conduct any notice-and-comment rulemaking. In May 2022, the Transportation Security Oversight Board ratified the security directive per the procedure specified in 49 U.S.C. § 114(l)(2). *See* Ratification of Security Directives, 87 Fed. Reg. 31093 (May 23, 2022).⁴

In June 2022, TSA modified the pipeline cybersecurity security directives in response to industry criticism. Industry critics believed that TSA had been non-transparent in not releasing the security directives for public comment and review. *See* Jonathan Greig, *TSA to change*

⁴ The Board is part of DHS and is comprised of certain cabinet level officials or their designees. *See* 49 U.S.C. § 115(b)(2).

cybersecurity rules for pipelines following industry criticism, The Record (June 28, 2022), tinyurl.com/4xhzbtjr. They also argued that the rules were overly prescriptive and, contrary to their purpose, damaged efforts to improve pipeline security. *See id.* A TSA spokesperson stated that TSA is committed to “working with the owners and operators of the nation’s critical transportation infrastructure” to defend those systems from the “ever-present threat of cyberattack.” *Id.*

VI. TSA Continually Expands The Scope Of Its Cybersecurity Regulatory Program And Repeatedly Renews It

In October 2022, TSA issued a second freight rail cybersecurity security directive, titled “Rail Cybersecurity Mitigation Actions and Testing,” and reissued the earlier “Enhancing Rail Cybersecurity” directive. App.9 (TSA, Security Directive 1580/82-2022-01, Rail Cybersecurity Mitigation Actions and Testing (Oct. 24, 2022), tinyurl.com/2s5n5h4k) (“Security Directive 1580/82-2022-01”); App.23 (TSA, Security Directive 1580-21-01A, Enhancing Rail Cybersecurity (Oct. 24, 2022), tinyurl.com/mr3k6eb3). The new Rail Cybersecurity Mitigation Actions and Testing security directive required covered railroad carriers to establish and implement a Cybersecurity Implementation Plan and establish a Cybersecurity Assessment

Program that would include submitting an annual plan to TSA to assess the effectiveness of cybersecurity measures and identify and resolve vulnerabilities. App.10–11 (Security Directive 1580/82-2022-01 at 2–3). The new security directive also required covered railroads to implement network segmentation policies, create access control measures, build continuous monitoring and detection procedures to detect cybersecurity threats, and apply timely security patches and updates for various systems. *Id.*

The new security directive did not state that there was any emergency such that TSA must act immediately. As before, the security directive cited “the ongoing cybersecurity threat to surface transportation systems.” App.9 (*Id.* at 1); *see also* App.125 (TSA, Action Memo re Issuing Security Directive 1580/82-2022-01: *Rail Cybersecurity Mitigation Actions and Testing*, and amending Security Directives 1580-2021-01: *Enhancing Rail Security* and 1582-2021-01: *Enhancing Public Transportation and Passenger Railroad Cybersecurity*, at 4 (Oct. 17, 2022)) (internal TSA memorandum purporting to justify security directive on basis of a determination that “Russia and China pose significant cyber threats to critical infrastructure, including freight and

passenger rail”). TSA indicated that cybersecurity threats targeting surface transportation have the *potential* for significant impacts on national security. App.126 (*Id.* at 5).

TSA’s public messaging was consistent with the lack of emergency, with the agency announcing in a press release that this security directive would “further enhance cybersecurity preparedness and resilience for the nation’s railroad operations.” App.132 (TSA, *TSA issues new cybersecurity requirements for passenger and freight railroad carriers* (Oct. 18, 2022), tinyurl.com/55tvmjb8). Like the security directive itself, the press release cited no emergency, pointing only to the “current threat environment.” App.133. TSA noted that this was the “latest in TSA’s performance-based security directives” and that TSA “intends to begin a rulemaking process.” *Id.*

In November 2022, TSA opened comment for an Advanced Notice of Proposed Rulemaking on surface-transportation cybersecurity. TSA, *Enhancing Surface Cyber Risk Management, Advance Notice of Proposed Rulemaking*, 87 Fed. Reg. 73527 (Nov. 30, 2022). The ANPRM sought “input regarding ways to strengthen cybersecurity and resiliency in the

pipeline and rail (including freight, passenger, and transit rail) sectors.”
Id. at 73527.

In October 2023, TSA once again renewed the parallel series of freight rail cybersecurity directives. App.33 (TSA, Security Directive 1580/82-2022-01A, Rail Cybersecurity Mitigation Actions and Testing (Oct. 24, 2023), tinyurl.com/22muytuj); App.49 (TSA, Security Directive 1580-21-01B, Enhancing Rail Cybersecurity (Oct. 24, 2023), tinyurl.com/2ws47ekk). TSA noted in a press release that the security directives’ requirements “seek to reduce the risk” that “cybersecurity threats pose.” App.150 (TSA, *TSA renews cybersecurity requirements for passenger and freight railroad carriers* (Oct. 23, 2023), tinyurl.com/4d98cyyu) (“TSA October 2023 Press Release”). The security directives, TSA again asserted, increased cybersecurity “preparedness.”
Id. TSA added a new requirement that owner/operators adopt a schedule for assessing at least one-third of the policies, procedures, measures and capabilities identified in their TSA-approved Cybersecurity Implementation Plan annually so that 100 percent will be assessed every three years. TSA reissued the Enhancing Rail Cybersecurity security directive in October 2024, and it remains in force. App.90 (TSA, Security

Directive 1580-21-01C, Enhancing Rail Cybersecurity (Oct. 24, 2024), tinyurl.com/2hks8a58).

In May 2024, meanwhile, TSA again reissued the Rail Cybersecurity Mitigation Actions and Testing security directive. App.56 (TSA, Security Directive 1580/82-2022-01B, Rail Cybersecurity Mitigation Actions and Testing (May 2, 2024)). TSA added significant new requirements, including mandating that covered railroads identify Positive Train Control systems as “Critical Cyber Systems.” App.57 (*Id.* at 2). Although industry had noted a series of concerns with these new requirements, *see* App.145–49 (Association of American Railroads White Paper), these concerns were never examined in notice and comment—TSA instead announced the reissued security directive, once again, in an email. CN petitioned for review of the May 2024 Security Directive. *See Grand Trunk Corp. v. TSA*, No. 24-2109 (7th Cir. filed June 28, 2024).

VII. TSA Issues The July 2024 Security Directive, Again Expanding Its Costly Cybersecurity Program Without Public Participation

Shortly after CN filed its challenge to the May 2024 Security Directive, TSA issued a new security directive styled as a “correction” to the challenged May 2024 Security Directive but keeping the May 2025

expiration date. See SA1 (TSA, Transmittal Memo re Issuance of SD 1580/82-2022-01C (July 1, 2024)); SA3 (TSA, Security Directive 1580/82-2022-01C, Rail Cybersecurity Mitigation Actions and Testing (July 1, 2024), tinyurl.com/4abtjh9w) (“July 2024 Security Directive” or the “Security Directive”). The July 2024 Security Directive states that it “supersedes” the May 2024 Security Directive.⁵

The July 2024 Security Directive contains an Authority line that reads: “AUTHORITY 49 U.S.C. 114(d), (f), (l) and (m).” SA3 (July 2024 Security Directive at 1). The Security Directive repeats that it is issued “due to the ongoing cybersecurity threat to surface transportation systems” and is intended to mitigate harm that “could result” from the “degradation, destruction, or malfunction” of surface-transportation systems. SA3 (*Id.* at 1). The Security Directive “continues to require”

⁵ The July 2024 Security Directive applies to Petitioners because it applies to “each freight railroad carrier identified in 49 C.F.R. § 1580.101.” SA3 (July 2024 Security Directive at 1). That regulation includes owner/operators “[d]escribed in § 1580.1(a)(1) of this part that is a Class I freight railroad,” and 49 C.F.R. § 1580.1(a)(1), in turn, includes “[e]ach freight railroad carrier that operates rolling equipment on track that is part of the general railroad system of transportation.” Grand Trunk and Illinois Central satisfy these criteria.

the “same” “cybersecurity measures first issued by TSA in October 2022.” SA3 (*Id.* at 1). Its “goal” is to “reduce the risk that cybersecurity threats pose to critical railroad operations and facilities.” SA4 (*Id.* at 2).

The Security Directive establishes and expands a sprawling and ongoing regulatory program, which agency staff have been actively implementing through regional offices. The Security Directive imposes a series of operational mandates on covered owner/operators’ internal cybersecurity practices. And the Security Directive requires covered railroads to submit to a perpetual regime of assessment and inspection by TSA.

First, the Security Directive requires owner/operators to create and implement a Cybersecurity Implementation Plan with specific measures and a schedule for achieving outcomes that TSA must review and approve. SA4 (*Id.* at 2). These outcomes include implementing network segmentation policies; establishing access control measures, such as multifactor authentication and memorized secret authenticator resets, including those for local and remote access; ensuring continuous monitoring and detection of cybersecurity threats, such as spam and

phishing emails and unauthorized code; and reducing the risk of exploitation of unpatched systems. SA7–11 (*Id.* at 5–9).

Second, covered owner/operators must develop a Cybersecurity Assessment Plan and submit it for TSA approval. Railroads must then use their Cybersecurity Assessment Plan to annually assess the measures in their Cybersecurity Implementation Plan, update their Cybersecurity Assessment Plan each year, and provide an annual report based on the Cybersecurity Assessment Plan’s assessment of the Cybersecurity Implementation Plan from the previous year. SA5 (*Id.* at 3).

Third, owner/operators must conduct an architecture design review of their networks within a year of approval of the Cybersecurity Implementation Plan, and the architecture design review must be updated every two years thereafter. SA11 (*Id.* at 9). Owner/operators must also ensure that at least one-third of the TSA-approved Cybersecurity Implementation Plan is assessed and audited every year, with 100 percent assessed over any three-year period. SA12 (*Id.* at 10).

In addition to reviewing and approving the Cybersecurity Implementation Plan and Cybersecurity Assessment Plan, TSA conducts

inspections to assess and verify covered owner/operators' implementation of the security controls in the Cybersecurity Implementation Plan across the owner/operator's Critical Cyber Systems. Railroads must maintain and provide detailed records to facilitate these inspections. App.162 (TSA, Frequently Asked Questions (FAQs) for TSA Security Directive 1580/82-2022-01 Series, Version 2.0, at 10, Question 21 (Sept. 27, 2024)). A violation of the Security Directive could subject an owner-operator to substantial civil penalties. *See* 49 USC § 114(u).

In addition to serially reissuing the freight rail cybersecurity directives with shifting and increasing requirements that require owner/operators to adjust to a new regulatory landscape each year, TSA has serially modified the compliance parameters of the security directives through sub-regulatory guidance, again without notice and comment. Most recently, TSA circulated FAQs for the Security Directive 1580/82-2022-01 series, an updated Informational Supplement for that series, and a Rail Cybersecurity Assessment Plan guide for best practices. App.152 (FAQs for Security Directive 1580/82-2022-01 Series); App.183 (TSA, Informational Supplement for TSA Security Directive 1580/82-2022-01 Series, Version 2.0 (Sept. 27, 2024)); App.262 (TSA, Rail

Cybersecurity Assessment Plan (CAP) Best Practice – Quick Reference Guide). Combined, these documents are in excess of 100 pages. This additional subregulatory guidance creates new requirements and adds to the complexity of the regulatory cybersecurity regime TSA has created without notice and comment.

All told, the July 2024 Security Directive imposes enormous costs. CN has already spent millions of dollars on cybersecurity tools and capabilities to comply with the July 2024 Security Directive and its predecessors, and CN estimates that it will spend millions more in ongoing compliance in years to come. CN has had to delay or put on hold four in-house cybersecurity projects in order to focus on compliance with the July 2024 Security Directive, diverting limited employee labor and other resources from addressing cyber threats. And these costs extend to the entire rail industry—TSA has estimated that compliance with its cyber risk management program would cost industry around \$100 million annually. Enhancing Surface Cyber Risk Management, Notice of Proposed Rulemaking, 89 Fed. Reg. 88488, 88535 (Nov. 7, 2024).

Despite these enormous costs, it is not clear that the July 2024 Security Directive provides any additional “enhancement of security.” 49

U.S.C. § 114(l)(3). As explained, CN and the entire freight rail industry have been successfully focused on cybersecurity since long before any security directive was issued. And TSA has never explained what additional benefit the security directives are expected to provide.

VIII. CN Files This Challenge To The July 2024 Security Directive

Because the July 2024 Security Directive states that it “supersedes” the May 2024 Security Directive that CN had already challenged, CN timely filed a Protective Petition for Review challenging the July 2024 Security Directive under a new case. *See Grand Trunk Corp. v. TSA*, No. 24-2156 (7th Cir. filed July 8, 2024). The following day, the Court consolidated the cases for purposes of briefing and disposition, and designated Case No. 24-2109 as the lead case.

On November 7, 2024, TSA issued a Notice of Proposed Rulemaking, proposing to impose cyber risk management requirements on rail owner/operators and other surface transportation industries. *Enhancing Surface Cyber Risk Management, Notice of Proposed Rulemaking*, 89 Fed. Reg. 88488 (Nov. 7, 2024). Comments are due in February 2025. The rulemaking will likely not be completed when the challenged July 2024 Security Directive expires in May 2025.

Additionally, TSA has told industry that it intends to again reissue the July 2024 Security Directive when it expires, as well as its other security directives. And materials in the administrative record suggest that TSA may reissue the July 2024 Security Directive without further Transportation Security Oversight Board approval. *See* AR672, AR677 (TSA Memos to Board) (requesting authorization “to extend the security directive beyond its current expiration date”).

SUMMARY OF ARGUMENT

TSA’s July 2024 Security Directive must be vacated for four independent reasons. *First*, TSA failed to provide notice and comment. *Second*, TSA failed to conduct a cost/benefit analysis. *Third*, TSA has not cited any substantive authority allowing it to impose the Security Directive’s micromanaging requirements. *Fourth*, the Security Directive is arbitrary and capricious because the requirements it imposes are untethered to the problem it purports to identify, and because TSA failed to explain its decisions to use its emergency procedures and to forego a cost/benefit analysis.

I. Plain statutory text requires TSA to provide notice and comment before issuing a regulation absent an “[e]mergency.” TSA concedes that

it promulgated the July 2024 Security Directive without notice and comment, and TSA has not pointed to anything that even plausibly could be deemed an emergency. TSA has instead cited “ongoing” and “ever-present” risks from Chinese and other attackers, but perpetual threats are not emergencies.

Section 114 makes clear that TSA may invoke Section 114(l)(2) only in extraordinary circumstances, not as a matter of course. Section 114(l) has two subsections: one that grants TSA regulatory authorization “[i]n general,” § 114(l)(1), and one that grants TSA regulatory authorization in “[e]mergencies,” § 114(l)(2). It is clear from that dichotomy that regulation under Section 114(l)(1) is the norm, and regulation under Section 114(l)(2) is the exception. Reinforcing that it is for emergencies only, Section 114(l)(2) applies only when the regulation “must” be issued “immediately” to protect transportation security. But TSA has invoked Section 114(l)(2) to establish an indefinite and iterative regulatory regime—one that at present has lasted for more than two years.

Because there is no emergency, the July 2024 Security Directive is unlawful and must be vacated.

II. Section 114(*l*)(3) provides that when “determining whether to issue ... a regulation under this section,” *i.e.*, Section 114(*l*), TSA must “consider ... whether the costs of the regulation are excessive in relation to the enhancement of security the regulation will provide.” TSA has conceded that it did not do that here, and the July 2024 Security Directive must be vacated for this independent reason as well.

III. When issuing the July 2024 Security Directive, TSA did not cite any statutory authority that allows it to impose the Security Directive’s requirements. Federal agencies may exercise only authority granted by statute. And Section 114 grants TSA only circumscribed authority over transportation security. TSA has not pointed to any statutory law that allows it to micromanage the freight rail industry’s internal cyber policies.

Most of the provisions the July 2024 Security Directive cites, all from Section 114, have no conceivable relation to freight rail cybersecurity, and none of the provisions give TSA regulatory authority over cybersecurity. For example, Subsection (f)(14) authorizes TSA to address security concerns on passenger flights by foreign airlines. Other provisions—such as one requiring TSA to develop plans for dealing with

threats to transportation security—direct TSA to take certain actions itself, not regulate industry. No provision authorizes TSA to regulate industry’s internal cybersecurity policies.

IV. TSA acted arbitrarily and capriciously by failing to tailor the Security Directive’s requirements to the purported threats it identifies. The July 2024 Security Directive cites generic state-sponsored cyber threats from Russia and China, yet requires all kinds of granular policies that it does not even attempt to link to these cyber threats. TSA also acted arbitrarily and capriciously by failing to explain why it invoked its emergency procedures or why it did not conduct a cost/benefit analysis.

STANDARD OF REVIEW

This Court has authority to “affirm, amend, modify, or set aside any part” of the Security Directive. 49 U.S.C. § 46110(c); *see also* 5 U.S.C. § 706 (“The reviewing court shall ... hold unlawful and set aside agency action ... found to be ... arbitrary [and] capricious [or] in excess of statutory jurisdiction, authority, or limitations”). This case primarily concerns questions of statutory interpretation. Courts resolving interpretive disputes “exercise independent judgment” to reach the text’s “best reading.” *Loper Bright Enters. v. Raimondo*, 144 S. Ct. 2244, 2262

(2024). To satisfy the arbitrary and capricious standard, meanwhile, agency action must be “reasonable and reasonably explained.” *FCC v. Prometheus Radio Project*, 592 U.S. 414, 423 (2021).

ARGUMENT

I. The July 2024 Security Directive Violates Section 114(l)’s Notice And Comment Rulemaking Requirement

This case presents a straightforward question of statutory interpretation: whether the “ongoing threat” of cybercrime existing in our world, SA4 (July 2024 Security Directive at 2), constitutes a perpetual “[e]mergency,” 49 U.S.C. § 114(l). The answer is no. There are always threats; there are not always emergencies. Because there is no emergency, TSA lacked authority to impose the Security Directive on freight railroads without notice and comment.

A. Section 114 Requires Rulemaking Absent An Emergency

The Supreme Court has “stressed over and over again in recent years” that statutory interpretation must “heed” “what a statute actually says.” *Groff v. DeJoy*, 600 U.S. 447, 468 (2023); *see also Loper Bright Enters.*, 144 S. Ct. 2244 (“best reading” controls). Section 114’s text makes clear that TSA may invoke Section 114(l)(2) only in extraordinary circumstances, not as a matter of course.

Section 114(*l*) has two subsections: the first grants TSA regulatory authorization “[i]n general,” § 114(*l*)(1), and the second grants TSA regulatory authorization in an “[e]mergency,” § 114(*l*)(2). These separate functions are clearly delineated in the heading for each subsection, and those plainly “are permissible indicators of the meaning of the text.” *Citizens Ins. Co. of Am. v. Wynndalco Enters., LLC*, 70 F.4th 987, 1002 n.10 (7th Cir. 2023); see A. Scalia & B. Garner, *Reading Law: The Interpretation of Legal Texts* 221 (2012) (“The title and headings are permissible indicators of meaning”). It is thus clear from the statutory dichotomy that regulation under Section 114(*l*)(1) “regulations” is the norm, and regulation under Section 114(*l*)(2) “[e]mergency procedures” is the exception.

Reinforcing that it is for emergencies only, Section 114(*l*)(2) applies only when the regulation “must” be issued “immediately” to protect transportation security. The term “must” denotes necessity, and the term “immediately” serious exigency. See *DirecTV, Inc. v. Barczewski*, 604 F.3d 1004, 1008 (7th Cir. 2010) (“good drafters use ‘must’ for mandates”); *Immediate*, Black’s Law Dictionary 897 (11th ed. 2019) (“Occurring without delay; instant.”). By coupling them together, the

drafters of Section 114(l)(2) showed that TSA may use its emergency procedures only when an emergency requires immediate action and not simply whenever the agency would prefer to avoid notice and comment.

Section 114(l)(2) further reinforces that emergency procedures are not for imposing years of regulation by providing that an emergency regulation “shall remain effective for a period not to exceed 90 days unless ratified or disapproved by the [Transportation Security Oversight] Board or rescinded by the Administrator.” 49 U.S.C. § 114(l)(B). That there is both a presumptive end point to emergency regulations and a possibility of early rescindment shows that the statute’s emergency procedures are not the norm, and not designed for a multi-year iterative process.

TSA, however, has flipped the statutory framework on its head. Without any justification or explanation, the agency has for years imposed a permanent and iterative regulatory regime on rail companies that reaches the minutiae of their internal cybersecurity procedures and implementation. That this cybersecurity program was never intended as a temporary measure is evident on the face of the successive Security Directives, which often contemplate future obligations extending

multiple *years*. *See, e.g.*, App.31 (TSA, Memo re: Renewal with revisions to SD 1580-82-2022-01 series: *Rail Cybersecurity Mitigation Actions and Testing*, at 2 (Oct. 23, 2023)) (“TSA-approved CIP are assessed each year so that 100 percent will be assessed every three years.”); SA5 (July 2024 Security Directive at 3) (“submit ... an annual update, for approval”; “submit ... an annual report that provides ... results from the previous year”). Meanwhile, TSA has never claimed that an emergency requires immediate regulation here. *Infra*.

To the contrary, TSA, remarkably, has taken the view that it may utilize Section 114(*l*)(2) as a matter of course. As the Government has recognized, “TSA regularly issues security directives without notice and comment.” TSA Supp. Br. 9, *Wall v. TSA*, No. 21-1220, 2023 WL 1830810 (D.C. Cir. Feb. 9, 2023) (TSA brief available at 2022 WL 4182503). Inexplicably, the Government has cited Section 114(*l*)(2) for the assertion that “TSA’s authority to issue security directives does not generally require notice-and-comment rulemaking.” *Id.* at 7. In reality, Section 114(*l*) says the opposite—TSA “[i]n general” must provide ordinary notice-and-comment process and only “[e]mergency” situations are excepted.

B. The July 2024 Security Directive Relies On A Threat, Not An Emergency

The July 2024 Security Directive does not even purport to cite an emergency. In sixteen pages, the Security Directive uses the word “emergency” one time, and that one instance is merely to note that the Transportation Security Oversight Board is required to review TSA’s emergency regulations.

TSA’s contemporaneous descriptions of its initial foray into regulating freight rail cybersecurity further belie any notion that its security directives have ever been premised on exigency. *See Dep’t of Com. v. New York*, 588 U.S. 752, 780 (2019) (“in reviewing agency action, a court is ordinarily limited to evaluating the agency’s contemporaneous explanation in light of the existing administrative record”); *Pension Benefit Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 654 (1990) (courts “evaluate the agency’s rationale at the time of decision”). For example, in a teleconference discussing the Security Directive’s first predecessor, a TSA senior official conceded that there was “no imminent or elevated

cyber threat” that “pertains to railroads.” App.99 (Industry Comments and Questions).⁶

TSA has never claimed that an emergency justifies its freight rail cybersecurity security directives. Because there is no emergency, the July 2024 Security Directive instead cites (at 2, SA4) “evolving intelligence” about the “growing sophistication” of “nefarious” actors that shows an “ongoing threat.” Those adjectives—“evolving,” “growing,” “ongoing”—connote perpetual risk, not acute exigency. Similarly, the Security Directive states (at 1, SA3) that it is needed to prevent “degradation” of rail infrastructure—“degradation” connotes gradual decay, not acute exigency. And when the Executive Branch has ratified prior iterations of the Security Directive, it has likewise described a “persistent cyber threat” but no emergency. Ratification of Security Directives, 88 Fed. Reg. 36921, 36922 (June 6, 2023); *see* Ratification of

⁶ As discussed in Section IV, *infra*, TSA’s failure to address this issue throughout its many iterations and expansions of the Security Directive renders it arbitrary and capricious.

Security Directives, 87 Fed. Reg. 31093, 31093 (May 23, 2022) (citing “this persistent threat”).⁷

That is consistent with how TSA has publicly described the July 2024 Security Directive. The Security Directive, as TSA repeatedly puts it, responds to the “persistent threat” of cybercrime and is an effort to “reduce ... risk.” *E.g.*, TSA, Transportation Security Timeline, *TSA Issues New Cybersecurity Requirements for Airport and Aircraft Operators*, tinyurl.com/r6az27r8 (last visited Nov. 24, 2024) (scroll to third “Mar. 2023” icon) (“TSA took this emergency action due to persistent cybersecurity threats against U.S. critical infrastructure.”); App.137 (TSA, *TSA issues new cybersecurity requirements for airport and aircraft operators* (Mar. 7, 2023), tinyurl.com/5xwt5kds) (“TSA is taking this emergency action because of persistent cybersecurity threats against U.S. critical infrastructure.”); App.134 (TSA, *The TSA Workforce Has Adapted to the Changing Threat Environment, Remains Steadfast and Committed to Securing the Nation’s Transportation Systems* (Oct. 27, 2022), tinyurl.com/y4e3d7xm) (referring to “the need to protect the

⁷ Despite the July 2024 Security Directive having remained in force well over 90 days, DHS has not published notice of its ratification.

United States from a range of persistent threats to our transportation network”). In the words of one TSA spokesperson, that threat is “ever-present.” Jonathan Greig, *TSA to change cybersecurity rules for pipelines following industry criticism*, *The Record* (June 28, 2022), tinyurl.com/4xhzbjtr.

That spokesperson is correct: the few threats the Security Directive cites are ever-present rather than sudden and acute. The Security Directive cites (at 2 n.4, SA4) “Russian state-sponsored and criminal cyber threats” (capitalization altered). The Security Directive cites (*id.*) a “China state-sponsored cyber actor living off the land” (capitalization and italics altered). And the Security Directive cites (*id.*) government websites covering general “information regarding current threats” but little or no information having anything to do with freight rail. The Security Directive unabashedly cites generalized threats that will exist continually.

C. A Threat Is Not An Emergency

Contrary to TSA’s position, an “ever-present” threat is not an “emergency.” *See Sorenson Commc’ns Inc. v. FCC*, 755 F.3d 702, 706–07 (D.C. Cir. 2014) (distinguishing between a “[c]ause for concern” and a

“crisis” because the former does not necessarily imply “exigency”). “[R]educ[ing] risk” with “preparedness,” App.150 (TSA October 2023 Press Release), may be a good idea but that does not reflect an emergency.

An “emergency” is something so unforeseen, infrequent, and unstable that it does not “admit of ... being dealt with according to rule.” Cong. Rsch. Serv., 98-505, *National Emergency Powers* 3 (2021); *see also*, *e.g.*, *Emergency*, *The American Heritage Dictionary of the English Language* 584 (4th ed. 2000) (an “emergency” is “a serious situation or occurrence that happens unexpectedly”); *Emergency*, *Cambridge Dictionary of American English* 279 (Sidney I. Landau 2000) (“a dangerous or serious situation, such as an accident, that happens suddenly or unexpectedly”); *Emergency*, *Black’s Law Dictionary* (12th ed. 2024) (“a sudden and serious event or an unforeseen change in circumstances that calls for immediate action to avert, control, or remedy harm”). The Supreme Court has characterized “emergency” in terms of urgency and relative infrequency of occurrence. *See, e.g.*, *Home Bldg. & Loan Ass’n v. Blaisdell*, 290 U.S. 398, 439 (1934). Examples include “a

great public calamity such as fire, flood, or earthquake.” *Id.* An emergency is definite, present, irregular, and acute.

A threat, by contrast, is indefinite, potentially realized in the future, and general. A threat is an “indication of an approaching menace” or “[a] person or thing that might well cause harm.” *Threat*, Black’s Law Dictionary (7th ed. 1999); *see also, e.g., Threat*, The New Oxford American Dictionary 1766 (Elizabeth J. Jewell & Frank Abate 2001) (“the possibility of trouble, danger, or ruin”); *Threat*, Cambridge Dictionary of American English 907 (Sidney I. Landau 2000) (“the possibility that something unwanted will happen”); *Threat*, Random House Webster’s College Dictionary 1362 (2000) (“an indication or warning of probable trouble”). The words “threat” and “emergency” are not interchangeable, and Section 114 uses one and not the other.

Cases applying analogous statutory provisions support this distinction. For example, the Occupational Safety and Health Act similarly permits the Occupational Safety and Health Administration to bypass notice and comment in an “emergency.” 29 U.S.C. § 655(c)(1). In holding that OSHA had overstepped that emergency authority, the Fifth Circuit recently explained that emergency procedures “are an unusual

response to exceptional circumstances,” and OSHA’s emergency power therefore “is an extraordinary power that is to be delicately exercised in only certain limited situations.” *BST Holdings, LLC v. OSHA*, 17 F.4th 604, 612 (5th Cir. 2021) (cleaned); *see also NFIB v. OSHA*, 595 U.S. 109, 114 (2022) (“emergency temporary standards ... are permissible ... only in the narrowest of circumstances”).

If an “ever-present” threat were an emergency, TSA rarely would need to provide notice and comment because it generally could invoke its emergency authority. As Congress well knew when enacting the Act in November 2001—a time of anthrax scares and murmurings of World War III—there are always significant threats for TSA to address. That was the whole point of creating the agency. But Congress provided that “in general” the normal notice-and-comment requirements apply, and only “emergency” situations are excepted.

Beyond TSA, federal statutory law grants other agencies emergency powers that they always could access—against Congress’s intent and in great tension with the Constitution—if they applied whenever there exists a persistent threat. For example, when the Federal Energy Regulatory Commission “determines that an emergency

exists,” it may commandeer private utility companies, requiring them to generate and transmit electric energy however FERC directs. *See* 16 U.S.C. § 824a(c)(1). During “any national emergency,” the President may “suspend the operation of provisions regulating the storage, transportation, disposal, procurement, handling, and testing of chemical and biological weapons,” including “the prohibition on testing such weapons on human subjects.” Amy L. Stein, *Energy Emergencies*, 115 *Nw. U. L. Rev.* 799, 883 n.119 (2020) (citing 50 U.S.C. § 1515). It is implausible that Congress intended agencies to hold these powers whenever there is an ever-present threat—that is to say, always—and the Constitution would not permit it.

Unfortunately, governments have a long history of abusing emergency power, and the United States government is not sinless on that score. “Executives have often used emergencies to circumvent the standard democratic or legal process.” Elena Chachko & Katerina Linos, *Emergency Powers for Good*, 66 *William & Mary L. Rev.* 4 (forthcoming 2024) (citing Anna Lührmann & Bryan Rooney, *Autocratization by Decree: States of Emergency and Democratic Decline*, 53 *Compar. Pol.* 617, 617–20 (2021)), *available at* tinyurl.com/mu754bn7; *see also* Max

Skonsberg, *Burke, A Man for All Seasons*, Law & Liberty (Aug. 5, 2024), tinyurl.com/47vhdrdw (“The conundrum that [Edmund] Burke often faced was how to prevent governments from using the pretext of continual emergencies to enlarge their authority over time.”). This case presents an example of the malady: TSA has distorted Section 114(l)(2) by using its emergency exception to impose permanent regulation. *See Cent. Forwarding, Inc. v. ICC*, 698 F.2d 1266, 1269–71 (5th Cir. 1983) (a regulation cannot “be described as an emergency measure” when it “is not a temporary measure” but rather “regulate[s] ... on a permanent basis”).

In recent years, the U.S. Supreme Court has repeatedly rejected federal agencies’ arguments that they may read a statute to take purportedly emergency action not actually tied to the purported emergency or clearly permitted by statute. For example, in 2020 the CDC, an agency tasked with preventing “communicable diseases,” invoked the Covid-19 pandemic to “impose[] a nationwide moratorium on evictions” in counties covering “[a]t least 80% of the country.” *Ala. Ass’n of Realtors v. HHS*, 594 U.S. 758, 759, 764 (2021). OSHA, “tasked with ensuring occupational safety,” imposed a vaccine mandate on

approximately 84.2 million employees. *NFIB*, 595 U.S. at 114. The Department of Education “canceled roughly \$430 billion of federal student loan balances” and “created a novel and fundamentally different loan forgiveness program” by invoking “a few narrowly delineated situations specified by Congress” and then “rewrit[ing] that statute from the ground up.” *Biden v. Nebraska*, 143 S. Ct. 2355, 2362, 2368, 2369 (2023). In each case, the Supreme Court held the agency’s appeal to emergency insufficient, and here TSA’s conduct reflects the same irreverence for the gravity of emergency power. Unlike in the prior cases, here the agency invoked its emergency authority and did not even assert the existence of an emergency.

D. The July 2024 Security Directive Establishes A Highly Prescriptive And Indefinite Regulatory Program That Demands Rulemaking

Especially when considered in conjunction with its prior and forthcoming iterations, the July 2024 Security Directive establishes a highly granular regulatory regime that normally would come through rulemaking after the agency has the benefit of notice and comment. TSA has emphasized the significance of threats to cybersecurity, but a

regulatory regime's importance is all the more reason for notice and comment.

That is true under the Act, common sense, and background principles of administrative law. Notice and comment “gives affected parties fair warning of potential changes in the law and an opportunity to be heard on those changes.” *Azar v. Allina Health Servs.*, 587 U.S. 566, 582 (2019). It also “affords the agency a chance to avoid errors and make a more informed decision.” *Id.*; see also, e.g., *Nw. Tissue Ctr. v. Shalala*, 1 F.3d 522, 531 (7th Cir. 1993) (“the parties ought to have a meaningful opportunity to present these materials to the agency before it embarks upon a course of action”); *Batterton v. Marshall*, 648 F.2d 694, 703 (D.C. Cir. 1980) (“The essential purpose of according ... notice and comment opportunities” “is to reintroduce public participation and fairness to affected parties after governmental authority has been delegated to unrepresentative agencies.”). Partly for those reasons, notice and comment is a bedrock norm in federal administrative law. See 5 U.S.C. § 553. And TSA agrees that when it promulgates rules pursuant to Section 114(l)(1), it must publish notice and provide interested persons with an opportunity to provide comment.

That the July 2024 Security Directive involves a “threat” does not alter that norm. Federal agencies routinely address severe and persistent threats through notice-and-comment rulemaking. *See, e.g.*, Medications for the Treatment of Opioid Use Disorder, Final Rule, 89 Fed. Reg. 7528 (Feb. 2, 2024) (HHS addressing opioid crisis public health emergency); Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, Notification of Availability, 84 Fed. Reg. 70435 (Dec. 23, 2019) (FEMA addressing threat of radiological incidents at commercial nuclear power plants). TSA itself addressed terror threats to domestic air transportation—the very concern that drove passage of the Act—through rulemaking. Passenger Screening Using Advanced Imaging Technology, Final Rule, 81 Fed. Reg. 11364 (Mar. 3, 2016). And FERC recently promulgated through notice-and-comment rulemaking a regulation addressing the cybersecurity threat to public utilities, demonstrating that whatever threat cybersecurity poses does not preclude notice and comment. *See* Incentives for Advanced Cybersecurity Investment, Final Rule, 88 Fed. Reg. 28348 (May 3, 2023) (FERC

addressing cybersecurity threat to public utilities). Emergency, not significant threat, is the basis for TSA bypassing notice and comment.

Further undermining any claim that the July 2024 Security Directive “must” be issued “immediately” is the fact that the Security Directive has existed in similar form for several years with incremental new and more requirements each year. *See* SA3 (July 2014 Security Directive at 1) (“This Security Directive continues to require the same performance-based cybersecurity measures first issued by TSA in October 2022.”). That is more than enough time for an agency to conduct a rulemaking. As explained, an “emergency” is something that does not “admit of ... being dealt with according to rule.” Cong. Rsch. Serv., 98-505, National Emergency Powers 3 (2021). But the cybersecurity mandates could have been dealt with according to rule this whole time.

E. Vacatur Is Required

TSA’s failure to provide notice and comment “is a fundamental flaw that normally requires vacatur.” *Nat. Res. Def. Council v. Wheeler*, 955 F.3d 68, 85 (D.C. Cir. 2020); *see Corner Post, Inc. v. Bd. of Governors of Fed. Rsrv. Sys.*, 144 S. Ct. 2440, 2463 (2024) (Kavanaugh, J., concurring) (“th[e] [Supreme] Court has affirmed countless decisions that vacated

agency actions, including agency rules”); *Johnson v. OPM*, 783 F.3d 655, 663 (7th Cir. 2015) (“[V]acatur is the presumptive remedy for a violation of the Administrative Procedure Act.”); *Ill. State Chamber of Com. v. EPA*, 775 F.2d 1141, 1151 (7th Cir. 1985) (vacating rule and remanding for notice and comment); *Chamber of Com. of U.S. v. SEC*, 88 F.4th 1115, 1118 & n.2 (5th Cir. 2023) (remand without vacatur is “not ... appropriate” for agency action “promulgated in violation of notice-and-comment requirements”). And vacatur is the remedy the Act authorizes. 49 U.S.C. § 46110(c) (authorizing this Court to “affirm, amend, modify, or set aside any part” of the Security Directive); see *Town of Barnstable, Mass. v. FAA*, 659 F.3d 28, 36 (D.C. Cir. 2011) (vacating agency action reviewed under 49 U.S.C. § 46110). This Court must vacate the Security Directive.

II. The July 2024 Security Directive Violates Section 114(l)’s Directive To Consider Costs And Benefits

TSA’s failure to conduct a statutorily required cost/benefit analysis is an independent reason the July 2024 Security Directive must be vacated. Section 114(l)(3) provides that when “determining whether to issue, rescind, or revise a regulation under this section,” *i.e.*, Section 114(l), TSA must “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.”

TSA has conceded that it did not consider costs here. *See* App.140 (Meeting Minutes at 2) (TSA senior official explaining to industry that “TSA does not do cost-benefit analysis for security directives.”). And the July 2024 Security Directive contains not one reference to costs. Even assuming TSA could lawfully impose the July 2024 Security Directive under Section 114(l)(2) (and it could not), the failure to conduct a cost/benefit analysis violates the Act—Section 114(l)(2), after all, is part of Section 114(l).

Section 114(l)(2) creates no exception to the cost/benefit requirement. Section 114(l)(2) states that TSA need not “provid[e] notice or an opportunity for comment” in an emergency “[n]otwithstanding any other provision of law or executive order (including an executive order requiring a cost-benefit analysis).” That does not modify the cost/benefit requirement—a notwithstanding clause does not add substantive content but rather shapes how the operative language that follows applies relative to other provisions by clarifying hierarchy. *See Cisneros v. Alpine Ridge Grp.*, 508 U.S. 10, 18 (1993) (“the use of such a

‘notwithstanding’ clause” “signals the drafter’s intention that the provisions of the ‘notwithstanding’ section override conflicting provisions of any other section”). Here, the notwithstanding clause simply provides that even when an executive order requires a cost/benefit analysis, TSA need not provide notice and comment in an emergency. (Under current law, regulatory action generally requires a cost/benefit analysis effectuated through notice and comment, *see* Improving Regulation and Regulatory Review, 76 Fed. Reg. 3821, 3822 (Jan. 18, 2011) (Executive Order 13563).) But that says nothing about the statutory requirement in Section 114(l)(3) that TSA must weigh costs against the anticipated security benefits. Nothing in Section 114(l)(2) can conceivably be read to excuse TSA from the Section 114(l)(3) cost/benefit requirement.

TSA’s failure to conduct the statutorily required cost/benefit analysis, therefore, is an independent reason the July 2024 Security Directive must be vacated. “Consideration of cost[s],” the Supreme Court has explained, “reflects the understanding that reasonable regulation ordinarily requires paying attention to the advantages and the disadvantages of agency decisions.” *Michigan v. EPA*, 576 U.S. 743, 753 (2015). And where, as here, the agency’s organic statute expressly

requires it to analyze the relationship of costs and benefits and the agency concedes that it did not do that, there can be no doubt that vacatur is required. *See, e.g., Interstate Nat. Gas Ass’n of Am. v. PHMSA*, 114 F.4th 744, 749, 754 n.6 (D.C. Cir. 2024) (“We vacate each of these standards based on PHMSA’s inadequate final cost-benefit analyses.”); *People of State of Ill. v. United States*, 666 F.2d 1066, 1075–77, 1083 (7th Cir. 1981) (vacating agency decision that failed to properly calculate costs); *Chamber of Com.*, 88 F.4th at 1118 (when a rule is promulgated “without observance of procedure as required by law,” “the default rule is that vacatur is the appropriate remedy” (cleaned)).

III. The July 2024 Security Directive Fails To Identify Any Grant Of Substantive Regulatory Authority Over Cybersecurity

TSA fails to identify any substantive grant of statutory authority that authorizes its venture into freight rail cybersecurity regulation. The Security Directive states that it “is issued under the authority of 49 U.S.C. 114(l)(2)(A).” SA3 (July 2014 Security Directive at 1 n.2). That subsection does not purport to grant TSA *any* substantive authority, let alone authority to launch a major cybersecurity regime. And the three

other subsections that TSA references in a memo header are equally unavailing. Vacatur is required.

A. Substantive Rulemaking Requires Substantive Authority

TSA's failure to identify a substantive basis for the July 2024 Security Directive is a fatal flaw. TSA "literally has no power to act" "unless and until Congress authorizes it to do so by statute." *FEC v. Cruz*, 596 U.S. 289, 301 (2022); *see also NFIB*, 595 U.S. at 117 ("Administrative agencies are creatures of statute. They accordingly possess only the authority that Congress has provided."). In the context of agency regulatory action, TSA must identify both a general grant of rulemaking authority and a specific grant of substantive authority.

Numerous cases recognize that an agency's "general rulemaking authority does not mean that the specific rule the agency promulgates is a valid exercise of that authority," *New York Stock Exch. LLC v. SEC*, 962 F.3d 541, 546 (D.C. Cir. 2020), and an agency's "general rulemaking authority plus statutory silence does not ... equal congressional authorization," *Merck & Co. v. HHS*, 385 F. Supp. 3d 81, 92 (D.D.C. 2019), *aff'd*, 962 F.3d 531 (D.C. Cir. 2020). For example, in *Alabama Association of Realtors v. HHS*, 594 U.S. 758 (2021), the Supreme Court

affirmed a district court’s vacatur of the CDC’s eviction moratorium. Although the Supreme Court never doubted the applicable statute authorized the agency to promulgate “regulations,” *id.* at 761 (citation omitted), it held that the statute’s substantive grant did not authorize the moratorium, *see id.* at 763–64. Here, TSA has invoked the “[e]mergency procedures” contained in Section 114(*l*)(2) but no substantive authority to impose the Security Directive’s hypertechnical cybersecurity regulatory requirements.

B. Section 114 Does Not Grant TSA Substantive Authority To Impose The Security Directive

As its purported authority, the July 2024 Security Directive cites subsections of Section 114 establishing TSA’s jurisdiction (Subsection (d)), generally defining TSA’s powers and duties (Subsections (f) and (m)), and authorizing TSA to issue regulations (Subsection (*l*)). But the Security Directive does not cite any substantive authority allowing TSA to regulate rail cybersecurity.

1. Subsection (d)

Subsection (d) merely states that TSA is “responsible for security in all modes of transportation.” That jurisdictional limit does not grant TSA authority to promulgate any particular regulation. *Cf. Ill. Citizens*

Comm. for Broad. v. FCC, 467 F.2d 1397, 1400 (7th Cir. 1972) (jurisdictional grant to FCC over radio communication did not allow it to halt building construction affecting radio reception). At most, Subsection (d) establishes that TSA cannot exercise responsibility for security *not* in a mode of transportation.

2. Subsection (f)

Most of Subsection (f) clearly has nothing to do with freight rail cybersecurity—for example, Subsection (f)(1) requires TSA to receive and assess transportation-related intelligence, and Subsection (f)(14) requires TSA to “address security concerns on passenger flights by foreign air carriers.”

The only provisions of Subsection (f) that arguably could relate to freight rail cybersecurity direct TSA to take certain actions itself, not regulate industry. Subsection (f) provides that TSA shall “assess threats to transportation,” “develop policies, strategies, and plans for dealing with threats to transportation security,” and “make other plans related to transportation security.” 49 U.S.C. § 114(f)(2)–(4). Subsection (f) also requires TSA to inspect security facilities and undertake research and development. § 114(f)(8)–(9). All of those authorizations require TSA to

act internally, not regulate the public. *Cf. DHS v. MacLean*, 574 U.S. 383, 395–96 (2015) (rejecting TSA interpretation of Section 114 because TSA “pushe[d] the statute too far” by arguing that Section 114’s instruction that TSA prescribe certain regulations also prohibited certain conduct by the public).

Only certain *other* provisions of Subsection (f)—that clearly have nothing to do with freight rail cybersecurity—authorize TSA to regulate the public. For example, Subsection (f)(12) directs TSA to “require background checks” for transportation-security personnel. A provision like that may authorize regulation of the private sector, but no regulation-authorizing provision in Subsection (f) concerns freight rail cybersecurity.

Finally, Subsection (f)(16) authorizes TSA to “carry out such other duties, and exercise such other powers, relating to transportation security as [TSA] considers appropriate, to the extent authorized by law.” That provision simply authorizes TSA to carry out existing “duties” and “powers” that are elsewhere “authorized by law.” *Id.* It does not create any powers or duties itself.

Moreover, interpreting that provision to allow TSA to promulgate any transportation-security rule that TSA deems “appropriate” would violate the nondelegation rule. The Constitution vests all of the United States’ legislative power in Congress. Under the nondelegation rule, Congress must determine the “important subjects” of a policy and may delegate only “those of less interest” to the executive “to fill up the details.” *Wayman v. Southard*, 23 U.S. (10 Wheat) 1, 20 (1825); *see also A.L.A. Schechter Poultry Corp. v. United States*, 295 U.S. 495, 529 (1935) (Congress may not “transfer to others” its legislative powers). And in those instances of delegation, “[t]he constitutional question is whether Congress has supplied an intelligible principle to guide the delegee’s use of discretion.” *Gundy v. United States*, 588 U.S. 128, 135 (2019). Under the intelligible-principle standard, “a delegation is permissible if Congress has made clear to the delegee ‘the general policy’ he must pursue and the ‘boundaries of his authority.’” *Id.* at 146 (cleaned).

An interpretation of Subsection 114(f)(16) allowing TSA to regulate transportation security however it “considers appropriate” would not provide an intelligible principle. It would not “ma[k]e clear” the “general policy” TSA must pursue and the “boundaries of [TSA’s] authority.” To

the contrary, it would provide no policy or boundaries at all, leaving all policymaking for TSA to legislate at its discretion. That would be unconstitutional. *See Pan. Refin. Co. v. Ryan*, 293 U.S. 388, 430 (1935) (Congress violates nondelegation rule when it “has declared no policy, has established no standard, has laid down no rule”). The Court should therefore reject a broad reading of Section 114(f). *See Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988) (“[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, the Court will construe the statute to avoid such problems.”).

In all events, TSA cursory citation to Subsection (f) (and Subsection (d) and Subsection (m)) in the memo header is unaccompanied by any explanation from TSA about why it believes the provisions relevant. SA3 (July 2024 Security Directive at 1). TSA’s less than “one sentence observation without argument is undeveloped and thus waived.” *United States v. Davis*, 29 F.4th 380, 385 n.2 (7th Cir. 2022); *see Neustar, Inc. v. FCC*, 857 F.3d 886, 894 (D.C. Cir. 2017) (agency forfeited legal argument by not making it in “the relevant agency orders”).

3. Subsection (l)

Subsection (l) provides a general grant of rulemaking authority (as well as the emergency procedures discussed above). It does not purport to confer any substantive regulatory authority. *Cf. Am. Forest & Paper Ass'n v. EPA*, 137 F.3d 291, 298 (5th Cir. 1998) (holding a provision of the Endangered Species Act merely imposes procedural requirements but “confers no substantive powers”); *Platte River Whooping Crane Tr. v. FERC*, 962 F.2d 27, 34 (D.C. Cir. 1992) (holding the same provision “does not expand the powers conferred on an agency by its enabling act”).

4. Subsection (m)

Subsection (m), titled “Personnel and Services,” concerns the apportionment of power within TSA. The provision authorizes TSA to manage itself but does not grant TSA any substantive regulatory authority over the public.

IV. The July 2024 Security Directive Is Not Tailored To The Purported Threats And Is Otherwise Arbitrary

The July 2024 Security Directive is arbitrary and capricious because it is not tailored to the threats it purports to identify and fails to address important aspects of the problem the government says it aims to address. Courts “cannot ignore the disconnect between [an agency’s]

decision made and the explanation given.” *Dep’t of Com.*, 588 at 785; see also *Motor Vehicle Mfrs. Ass’n of U.S. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

First, the July 2024 Security Directive is premised on purported threats from state-sponsored actors targeting U.S. Government and private-sector networks in general (though not freight rail specifically). See SA4 n.4 (July 2014 Security Directive at 2 n.4) (invoking generalized threats from Russian and Chinese state-sponsored actors against critical infrastructure). But the Security Directive is not directly responsive to such general purported threats and indeed reaches far beyond them by micromanaging covered companies’ internal cybersecurity practices in myriad ways.

For example, covered companies are required to designate Positive Train Control as a Critical Cyber System under the July 2024 Security Directive, which in turn triggers applicability of the Security Directive’s requirements to those systems. SA7–8 (*Id.* at 5–6). And though the freight rail industry previously explained to TSA that Positive Train Control is comprised of many separate subsystems that should not be treated as a single entity, App.145–46 (Association of American Railroads

White Paper), the agency did not grapple with the issues raised by treating Positive Train Control in this way, and the July 2024 Security Directive broadly regulates Positive Train Control.

The July 2024 Security Directive also requires measures to address myriad discrete cybersecurity issues such as spam and phishing emails; communications with malicious IP addresses, malicious web domains and applications; unauthorized code executions; malicious command and control servers; and unpatched systems. SA10–11, 17–18 (July 2024 Security Directive at 8–9, 15–16). It also requires broad network segmentation policies that require encryption of all content flowing between operational systems and IT systems. SA8 (July 2024 Security Directive at 6). The required access control measures are sometimes specific—for example multi-factor authentication and password resets—but often they extend into broad and vague standards on managing shared accounts, access rights, and domain trust relationships. SA9 (*Id.* at 7). The July 2024 Security Directive’s continuous monitoring and detection policies also entail burdensome cybersecurity incident logging and investigation policies. SA10–11 (*Id.* at 8–9). Each of these may be good ideas for network operators and common features of cyber risk

management programs. But the TSA's burdensome mandates about each are not tailored to, and extend far beyond, any identified threat.

Second, the July 2024 Security Directive never addresses TSA's departure from Section 114(l)'s requirements that TSA conduct notice and comment rulemaking and consider whether the costs of the Security Directive are excessive in relation to any security enhancement. In addition to violating the statute, these failures show TSA was not engaged in reasoned decisionmaking.

The Class I freight railroads proactively raised the rulemaking issue to TSA when they first learned that the agency planned to regulate them using its emergency procedures, pointing out that a TSA senior official conceded that there was "no imminent or elevated cyber threat" that "pertains to railroads." App.99 (Industry Comments and Questions). TSA's contemporaneous response overlooks this important industry input, *see* App.113–14 (TSA, Responses to Industry Comments re SDs 1580-21-01 and 1582-21-01), showing TSA "entirely failed to consider [this] important aspect of the problem." *Boucher v. USDA*, 934 F.3d 530, 547 (7th Cir. 2019) (quoting *State Farm*, 463 U.S. at 43). At a minimum,

the agency failed to “articulate a satisfactory explanation for its action.”

Id. (cleaned).

The same is true for the cost/benefit analysis. Again, industry reminded the agency through the limited mechanisms that were available to it outside of rulemaking what it is that the statute plainly requires. Again, TSA believed it need not comply but did not explain why. *See* App.140 (Meeting Minutes at 2) (TSA senior official asserting that “TSA does not do cost-benefit analysis for security directives”). And again, because reasoned decisionmaking requires at least an explanation when an important issue is presented to the agency, *see State Farm*, 463 U.S. at 43, TSA’s refusal to provide one was arbitrary and capricious.

CONCLUSION

This Court should vacate the July 2024 Security Directive.

Respectfully Submitted,

/s/ Jeremy J. Broggi

Megan L. Brown

Jeremy J. Broggi

Jacqueline F. Brown

Michael J. Showalter

WILEY REIN LLP

2050 M Street NW

Washington, DC 20036

Phone: (202) 719-7000

mbrown@wiley.law

jbroggi@wiley.law

jfbrown@wiley.law

mshowalter@wiley.law

Counsel for Petitioners

November 27, 2024

CERTIFICATE OF COMPLIANCE

I hereby certify, on November 27, 2024, that:

1. This document complies with the word limit under Circuit Rule 32(c) because this document contains 12,483 words.

2. This document complies with the typeface requirements and the type-style requirements of Circuit Rule 32(b) because this document was prepared in a proportionally spaced typeface using Microsoft Word for Office 365 MSO in a 14-point Century Schoolbook font.

/s/ Jeremy J. Broggi

Jeremy J. Broggi

CERTIFICATE OF SERVICE

I certify that on November 27, 2024 a true and correct copy of this Brief was filed and served electronically upon counsel of record registered with the Court's CM/ECF system.

/s/ Jeremy J. Broggi

Jeremy J. Broggi

CIRCUIT RULE 30(d) CERTIFICATE

In accordance with Circuit Rule 30(d), I hereby certify that all materials required by Circuit Rules 30(a) and (b) are included in the Required Short Appendix bound with Petitioners' Principal Brief and the concurrently filed Appendix.

/s/ Jeremy J. Broggi

Jeremy J. Broggi

SHORT APPENDIX

TABLE OF CONTENTS

Transmittal Memo Re Issuance of SD 1580-82-2022-01C
dated July 1, 2024.....SA1

SD 1580-82-2022-01C,
Rail Cybersecurity Mitigation Actions and Testing
dated July 1, 2024.....SA3



U.S. Department of Homeland Security
Transportation Security Administration
 6595 Springfield Center Drive
 Springfield, Virginia 20598

MEMORANDUM

To: Covered Railroad Owner/Operators

Date: July 1, 2024

Subject: Issuance of Security Directive 1580/82-2022-01C: *Rail Cybersecurity Mitigation Actions and Testing*

Attached to this memorandum is Security Directive 1580/82-2022-01C, *Rail Cybersecurity Mitigation Actions and Testing*. Based on industry feedback TSA is issuing this correction to the most recent revision to the Security Directive 1580/82-2022-01 series, which took effect on May 2, 2024, and expires May 2, 2025. The expiration date is not affected by this correction.

This security directive series applies to each freight railroad carrier identified in 49 CFR § 1580.101 and other TSA-designated freight and passenger railroads. If TSA revises the applicability of the Security Directive 1580/82-2022-01 series in the future by designating additional railroad Owner/Operators, TSA will notify these Owner/Operator(s) and provide specific compliance deadlines for the requirements in this security directive.

The issuance of this security directive maintains TSA's performance-based cybersecurity requirements, which were first issued in October 2022, and includes limited revisions. This correction adds the definition of "business critical functions" and clarifies the application of the alternate methods of securing positive train control (PTC) system components in locomotives in Section III.C.6.

The security directive changes are summarized in the table below.

Section III.C.6.

This **revised section** clarifies that Owner/Operators subject to 49 CFR 232.105(h)(1-4) (General requirements for locomotives), 49 CFR 236.3 (Locking of signal apparatus housings), *or* 49 CFR 236.553 (Seal, where required) may, for PTC hardware and software components installed on freight and passenger locomotives of the PTC system, rely on the physical security measures used to comply with these requirements, as applicable, in lieu of implementing the requirements in Section III.C.1.-5. of this security directive. Owner/Operators must specify in their Cybersecurity Implementation Plan what physical security measures it uses to prevent unauthorized access to PTC components installed on locomotives. This alternative only applies to the components identified in this paragraph.

Section VII.

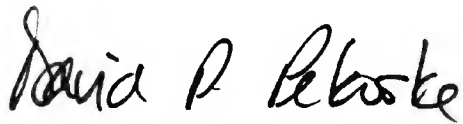
This **revised section** adds a definition for *business critical functions*, which was unintentionally omitted from Security Directive 1580/82-2022-01B. For the purpose of this security directive

AR621

series, *business critical functions* means the Owner/Operator's determination of capacity or capabilities to support functions necessary to meet operational needs and supply chain expectations. The use of this term within the context of "operational disruption" is not intended to change the scope of which systems must be identified as critical.

Consistent with TSA's previous determination, this security directive is not marked as Sensitive Security Information (SSI). While security directives generally are categorically deemed SSI under TSA's regulations (49 CFR part 1520), TSA previously determined that the contents of this security directive would not be detrimental to transportation security if publicly disclosed. No revisions to the Information Collection Request previously approved by the Office of Management and Budget are necessary to accommodate any information collected under the revision.

The security directive requires that railroad Owner/Operators provide written confirmation of receipt via email to SurfOpsRail-SD@tsa.dhs.gov. All queries concerning the attached security directive should be submitted to TSA at TSA-Surface@tsa.dhs.gov.



David P. Pekoske
Administrator
Transportation Security Administration

Attachment: Security Directive 1580/82-2022-01C



<u>NUMBER</u>	Security Directive 1580/82-2022-01C
<u>SUBJECT</u>	Rail Cybersecurity Mitigation Actions and Testing
<u>EFFECTIVE DATE</u>	July 1, 2024
<u>EXPIRATION DATE</u>	May 2, 2025
<u>SUPERSEDES</u>	Security Directive 1580/82-2022-01B
<u>APPLICABILITY</u>	Each freight railroad carrier identified in 49 CFR 1580.101 and other TSA-designated freight and passenger railroads
<u>AUTHORITY</u>	49 U.S.C. 114(d), (f), (l) and (m)
<u>LOCATION</u>	All locations within the United States

I. PURPOSE AND GENERAL INFORMATION

The Transportation Security Administration (TSA) is issuing this Security Directive due to the ongoing cybersecurity threat to surface transportation systems and associated infrastructure to mitigate the significant harm to the national and economic security of the United States that could result from the “degradation, destruction, or malfunction of systems that control this infrastructure.”¹

This Security Directive continues to require the same performance-based cybersecurity measures first issued by TSA in October 2022.² The actions required by TSA 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.³ Even minor disruptions in critical rail systems may result in temporary product shortages that can cause significant harm to national security. Prolonged disruptions in the flow of commodities could lead to widespread supply chain disruptions, with ripple effects across the economy. Disruptions and delays may affect industries that depend on the commodities transported by the nation’s railroads.

¹ See *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems* (July 29, 2021).

² As noted in the Office of Management and Budget’s Unified Agenda, TSA intends to more permanently codify these requirements through rulemaking.

³ This Security Directive is issued under the authority of 49 U.S.C. 114(l)(2)(A), which states: “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.”

The goal of this Security Directive is to reduce the risk that cybersecurity threats pose to critical railroad operations and facilities through implementation of layered cybersecurity measures that provide defense-in-depth. 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.⁴

In general, this Security Directive is applicable to the same railroads subject to the Security Directive 1580-21-01 series, “Enhancing Rail Cybersecurity,”⁵ and additional TSA-designated freight and passenger railroads notified by TSA based on a risk determination. All revisions to this Security Directive series from the previous version, SD 1580/82-2022-01B, are highlighted in bold.

To protect against the ongoing threat to the United States’ national and economic security, this Security Directive mandates that these railroad Owner/Operators implement the following cybersecurity measures to prevent disruptions to their infrastructure and/or operations. Specifically, Owner/Operators must:

1. Establish and implement a TSA-approved Cybersecurity Implementation Plan that describes the specific measures employed and the schedule for achieving the following outcomes, as more fully described in Section III.A through III.E.:
 - a. Implement network segmentation policies and controls to ensure that the Operational Technology system can continue to safely operate in the event that an Information Technology system has been compromised;
 - b. Implement access control measures to secure and prevent unauthorized access to Critical Cyber Systems;
 - c. Implement continuous monitoring and detection policies and procedures to detect cybersecurity threats and correct anomalies that affect Critical Cyber System operations; and
 - d. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on Critical Cyber Systems in a timely manner using a risk-based

⁴ See Joint Cybersecurity Advisory (AA22-110A), Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure (dated April 20, 2022), available at https://www.cisa.gov/uscrt/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf. Additional information regarding current threats is posted at <https://www.cisa.gov/shields-up>. See also Office of the Director of National Intelligence (ODNI), *Annual Threat Assessment of the U.S. Intelligence Community* (dated February 6, 2023), available at [2023 Annual Threat Assessment of the U.S. Intelligence Community](https://www.odni.gov/2023-annual-threat-assessment-of-the-u-s-intelligence-community); and CISA Joint Cybersecurity Advisory: *People’s Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection* (AA23-144a) (dated May 24, 2023), available at <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a>.

⁵ See Section II.A. of this Security Directive for applicability.

methodology.

2. Develop a Cybersecurity Assessment Plan and submit (a) an annual update, for approval, that describes how the Owner/Operator will proactively and regularly assess the effectiveness of cybersecurity measures, and identify and resolve device, network, and/or system vulnerabilities, and (b) an annual report that provides Cybersecurity Assessment Plan results from the previous year. *See* Section III.F.

All currently-identified railroad Owner/Operators have submitted a Cybersecurity Implementation Plan and are awaiting TSA approval or have a TSA-approved Cybersecurity Implementation Plan in place. This plan sets the security measures and requirements against which TSA inspects for compliance. *See* Section II.B.

This revision clarifies **the application of the alternate methods of securing positive train control (PTC) system components in locomotives. This revision also includes a definition for “business critical functions” because the revised definition of “operational disruption” removed the term “necessary capacity” and replaced it with “business critical functions.”**

Pursuant to 49 U.S.C. 114(f), the TSA Administrator is authorized to “enforce security-related regulations and requirements”; “inspect, maintain, and test security facilities, equipment, and systems”; and “oversee the implementation, and ensure the adequacy of security measures at ... transportation facilities.” Given this authority, TSA may require Owner/Operators to provide specific documentation and access to TSA as necessary to establish compliance. *See* Section IV. of this Security Directive for examples of the type of records to which TSA may require access. Although TSA has determined that this document is not Sensitive Security Information (SSI), all information that must be reported or submitted to TSA pursuant to this Security Directive is SSI subject to the protections of part 1520 of title 49, Code of Federal Regulations. The Department of Homeland Security may use the information, with company-specific data redacted, for Department of Homeland Security’s intelligence-derived reports. TSA and the Cybersecurity and Infrastructure Security Agency also may use information submitted for vulnerability identification, trend analysis, or to generate anonymized indicators of compromise or other cybersecurity products to prevent other cybersecurity incidents.⁶ Information provided to Department of Homeland Security pursuant to this Security Directive may also be shared with other agencies as appropriate.⁷ The distribution, disclosure, and availability of information will be

⁶ *See* OMB Control No. 1670-0037.

⁷ Presidential Policy Directive (PPD) 41 requires Federal agencies to rapidly share incident information with each other to achieve unity of governmental effort. *See* PPD-41 § III.D (“Whichever Federal agency first becomes aware of a cyber incident will rapidly notify other relevant Federal agencies in order to facilitate a unified Federal response and ensure that the right combination of agencies responds to a particular incident”). Furthermore, for purposes of information shared with the Department of Homeland Security pursuant to this directive, cyber incident responders with responsibilities under PPD-41 are “covered” persons with a “need to know,” as provided by 49 CFR 1520.7 and 1520.11, respectively.

restricted to persons with a need to know, and safeguarding, protecting, and marking methods for sensitive/critical information will be utilized.⁸ The Office of Management and Budget (OMB) has approved this collection under OMB Control No. 1652-0074.

TSA will seek review and ratification of this Security Directive by the Transportation Security Oversight Board (TSOB). The TSOB is statutorily required to “review and ratify or disapprove” emergency regulations and security directives issued by TSA under 49 U.S.C. 114(l)(2). *See* 49 U.S.C. 114(l)(2)(B) and 115(c)(1). If the TSOB decides not to ratify any section or subsection of this Security Directive, or deems any section or subsection inapplicable, the remainder of this Security Directive shall not be affected unless otherwise specified by the TSOB.

II. ACTIONS REQUIRED

A. Applicability, Deadlines for Compliance, and Scope

1. *Applicability*: The provisions of this Security Directive apply to the following Owner/Operators:
 - a. Freight Railroad Owner/Operators subject to applicability described in 49 CFR 1580.101.
 - b. *Other TSA-designated Freight and Passenger Railroad Owner/Operators*: If TSA identifies additional railroad Owner/Operators who were not already subject to the Security Directive 1580/82-2022-01 series, TSA will notify these Owner/Operator(s) and provide specific compliance deadlines for the requirements in this Security Directive.
2. *Managed Security Service Providers*. If an Owner/Operator has delegated to, or shared responsibility with, a Managed Security Service Provider, wholly or in part, for specific security measures in the Owner/Operator’s Cybersecurity Implementation Plan, the Owner/Operator retains sole responsibility under this Security Directive for ensuring compliance with the Owner/Operator’s TSA-approved Cybersecurity Implementation Plan and this Security Directive.
3. *Authorized Representative*. Authorized Representatives are empowered by the Owner/Operator to coordinate and/or conduct activities required by this Security Directive and/or contained within the Owner/Operator’s TSA-approved Cybersecurity Implementation Plan. Both Owner/Operators and Authorized Representatives are liable for non-compliance on the part of the Authorized Representative with the applicable requirements of the Owner/Operator’s TSA-approved Cybersecurity Implementation Plan and this Security Directive.

⁸ *See* 49 CFR 1520.5(b)(5) and <https://www.tsa.gov/for-industry/sensitive-security-information>.

4. *Scope:* The requirements in this Security Directive apply to Critical Cyber Systems of TSA-designated freight and passenger railroads.

Note: If an Owner/Operator determines they have no Critical Cyber Systems, as defined in Section VII. of this Security Directive, they must notify TSA in writing within 60 days of the effective date of this Security Directive. TSA will notify the Owner/Operator if the agency disagrees with the Owner/Operator's determination and may require the Owner/Operator to provide additional information regarding the methodologies or rationale used to identify Critical Cyber Systems. After consultation with the Owner/Operator, TSA may notify an Owner/Operator that it must include Critical Cyber Systems identified by TSA in its Cybersecurity Implementation Plan. In the event that an Owner/Operator's method of operation changes, they must reevaluate whether they have a Critical Cyber System, and if so, notify TSA within 60 days of the change in operations to determine the schedule for complying with the requirements of this Security Directive.

B. Cybersecurity Implementation Plan

1. The Cybersecurity Implementation Plan must provide all the information required by Sections III.A. through III.E. of this Security Directive and describe in detail the Owner/Operator's defense-in-depth plan, including physical and logical security controls, for meeting each of the requirements in Sections III.A. through III.E.
2. Once approved by TSA, the Owner/Operator must implement and maintain all measures in the TSA-approved Cybersecurity Implementation Plan in accordance with the schedule as stipulated in the plan.

III. CYBERSECURITY MEASURES

The Owner/Operator must:

- A. Identify the Owner/Operator's Critical Cyber Systems as defined in Section VII. of this Security Directive.
 1. TSA will notify the Owner/Operator if the agency disagrees with the Owner/Operator's determination and may require the Owner/Operator to provide additional information regarding the methodologies or rationale used to identify Critical Cyber Systems. After consultation with Owner/Operators, TSA may notify an Owner/Operator that it must include additional Critical Cyber Systems identified by TSA not previously identified by the Owner/Operator in their Cybersecurity Implementation Plan.
 2. Positive Train Control (PTC) Systems
 - a. Owner/Operators who are either required to install and operate PTC under 49 CFR part 236, subpart I, and/or voluntarily install and operate PTC under CFR part 236, subpart H or I, must include PTC systems as a Critical Cyber System.

AR609

- b. Any Owner/Operator required to include PTC systems under Section III.A.2.a. who has not previously identified these systems as a Critical Cyber System, must submit an updated Cybersecurity Implementation Plan to TSA for approval no later than 60 days after the effective date of this Security Directive.
- B. Implement network segmentation policies and controls designed to prevent operational disruption to the Operational Technology system if the Information Technology system is compromised or vice-versa. As applied to Critical Cyber Systems, these policies and controls must include:
 1. A list and description of—
 - a. Information Technology and Operational Technology system interdependencies;
 - b. All external connections to the Information Technology and Operational Technology system;
 - c. Zone boundaries, including a description of how Information Technology and Operational Technology systems are defined and organized into logical zones based on criticality, consequence, and operational necessity; and
 - d. Policies to ensure Information Technology and Operational Technology system services transit the other only when necessary for validated business or operational purposes.
 2. An identification and description of measures for securing and defending zone boundaries, that includes security controls—
 - a. To prevent unauthorized communications between zones; and
 - b. To prohibit Operational Technology system services from traversing the Information Technology system, and vice-versa, unless the content is encrypted or, if not technologically feasible, otherwise secured and protected to ensure integrity and prevent corruption or compromise while the content is in transit.
- C. Implement access control measures, including those for local and remote access, to secure and prevent unauthorized access to Critical Cyber Systems. Except as provided in Section III.C.6., these measures must incorporate the following policies, procedures, and controls:
 1. Identification and authentication policies and procedures designed to prevent unauthorized access to Critical Cyber Systems that include—

- a. A policy for memorized secret authenticators resets that includes criteria for when resets must occur;⁹ and
 - b. Documented and defined mitigation measures for components of Critical Cyber Systems that will not fall under the policy required by the preceding subparagraph (III.C.1.a), and a timeframe to complete these mitigations.
2. Multi-factor authentication, or other logical and physical security controls that supplement password authentication to provide risk mitigation commensurate to multi-factor authentication. If an Owner/Operator does not apply multi-factor authentication for access to Operational Technology components or assets, the Owner/Operator must specify what compensating controls are used to manage access.
3. Policies and procedures to manage access rights based on the principles of least privilege and separation of duties. Where not technically feasible to apply these principles, the policies and procedures must describe the compensating controls that the Owner/Operator will apply.
4. Enforcement of standards that limit the availability and use of shared accounts to those that are critical for operations, and then only if absolutely necessary. When the Owner/Operator uses shared accounts for operational purposes, the policies and procedures must ensure—
 - a. Access to shared accounts is limited through account management that uses principles of least privilege and separation of duties; and
 - b. Individuals who no longer need access do not have knowledge of the password necessary to access the shared accounts.
5. Regularly updated schedule for review of existing domain trust relationships to ensure their necessity and establish policies to manage these relationships.
6. For the PTC hardware and software components installed on freight and passenger locomotives of the PTC system, Owner/Operators subject to the requirements of **49 CFR 232.105(h)(1-4) (General requirements for locomotives)**, 49 CFR 236.3 (Locking of signal **apparatus** housings), or 49 CFR 236.553 (Seal, where required) may rely on **the physical security measures used to comply with these requirements, as applicable**, in lieu of implementing the requirements in Sections III.C.1.-5. of this Security Directive. The Owner/Operator must specify in its Cybersecurity Implementation Plan what physical security measures it uses to prevent unauthorized access to PTC components **installed on locomotives. This alternative only applies to the components identified in this paragraph.**

⁹ This policy should be compliant with the most current version of the National Institute of Standards and Technology's Special Publication 800-63, Digital Identity Guidelines (available at <https://csrc.nist.gov/publications/detail/sp/800-63/3/final>).

- D. Implement continuous monitoring and detection policies and procedures that are designed to prevent, detect, and respond to cybersecurity threats and correct anomalies affecting Critical Cyber Systems. These measures must include:
1. Capabilities to—
 - a. Defend against malicious email, such as spam and phishing emails, to preclude or mitigate against adverse impacts to operations;
 - b. Block ingress and egress communications with known or suspected malicious Internet Protocol addresses;
 - c. Control impact of known or suspected malicious web domains or web applications, such as by preventing users and devices from accessing malicious websites;
 - d. Block and prevent unauthorized code, including macro scripts, from executing; and
 - e. Monitor and/or block connections from known or suspected malicious command and control servers (such as Tor exit nodes, and other anonymization services).
 2. Procedures to—
 - a. Audit unauthorized access to internet domains and addresses;
 - b. Document and audit any communications between the Operational Technology system and an external system that deviates from the Owner/Operator's identified baseline of communications;
 - c. Identify and respond to execution of unauthorized code, including macro scripts; and
 - d. Implement capabilities (such as Security, Orchestration, Automation, and Response) to define, prioritize, and drive standardized incident response activities.
 3. Logging policies that—
 - a. Require continuous collection and analyzing of data for potential intrusions and anomalous behavior on Critical Cyber Systems and other Operational and Information Technology systems that directly connects with Critical Cyber Systems; and
 - b. Ensure data is maintained for sufficient periods, to provide effective investigation of cybersecurity incidents.

4. Mitigation measures or manual controls to ensure industrial control systems can be isolated when a cybersecurity incident in the Information Technology system creates risk to the safety and reliability of the Operational Technology system.¹⁰
- E. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers, and firmware on Critical Cyber Systems consistent with the Owner/Operator's risk based methodology. These measures must include:
1. A patch management strategy that ensures all critical security patches and updates on Critical Cyber Systems are current.
 2. The strategy required by Section III.E.1. must include:
 - a. The risk methodology for categorizing and determining criticality of patches and updates, and an implementation timeline based on categorization and criticality; and
 - b. Prioritization of all security patches and updates on the Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities Catalog.¹¹
 3. If the Owner/Operator cannot apply patches and updates on specific Operational Technology systems without causing a severe degradation of operational capability, the patch management strategy must include a description and timeline of additional mitigations that address the risk created by not installing the patch or update.
- F. Develop a Cybersecurity Assessment Plan.
1. The Owner/Operator must develop a Cybersecurity Assessment Plan for proactively assessing Critical Cyber Systems to ascertain the effectiveness of cybersecurity measures and to identify and resolve device, network, and/or system vulnerabilities.
 2. The Cybersecurity Assessment Plan required by Section III.F.1. must—
 - a. Assess the effectiveness of the Owner/Operator's TSA-approved Cybersecurity Implementation Plan;
 - b. Include a cybersecurity architecture design review to be conducted within the first 12 months after the Cybersecurity Implementation Plan approval and at least once every two years thereafter. A cybersecurity architecture design review contains verification and validation of network traffic, a system log review, and analysis to

¹⁰ See related requirement in Section D.1.a. in the SD 1580-21-01 series.

¹¹ Available at: <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.

- identify cybersecurity vulnerabilities related to network design, configuration, and inter-connectivity to internal and external systems;
- c. Incorporate other assessment capabilities designed to identify vulnerabilities based on evolving threat information and adversarial capabilities, such as penetration testing of Information Technology systems, including the use of “red” and “purple” team (adversarial perspective) testing;
 - d. Include a schedule for assessing and auditing specific cybersecurity measures and/or actions required by subparagraphs F.2.a. through F.2.c. of this section. The schedule must ensure that at least one-third (1/3) of the policies, procedures, measures, and capabilities in the TSA-approved Cybersecurity Implementation Plan are assessed each year, with 100 percent assessed over any three-year period; and
 - e. Ensure an annual report of the results of assessments conducted in accordance with the Cybersecurity Assessment Plan is submitted to TSA as described in paragraph F.4. of this section. The required report must indicate—
 - i. For the previous 12 months, which assessment method(s) were used to determine whether the policies, procedures, and capabilities described by the Owner/Operator in its Cybersecurity Implementation Plan are effective; and
 - ii. Results of the individual assessments conducted in the previous 12 months.
3. The Owner/Operator must comply with the following deadlines for submitting the Cybersecurity Assessment Plan, annual updates, and annual reports.
- a. No later than 60 calendar days after TSA’s approval of the Owner/Operator’s Cybersecurity Implementation Plan, the Owner/Operator must submit its initial Cybersecurity Assessment Plan to TSA, for approval.
 - b. The Owner/Operator must review and update its Cybersecurity Assessment Plan on an annual basis and submit it to TSA for approval. The first annual update must be submitted to TSA for approval no later than 12 months from the date the Owner/Operator *submitted* its first Cybersecurity Assessment Plan to TSA as required by this Security Directive. All subsequent annual updates must be submitted to TSA no later than 12 months from the date of TSA’s *approval* of the Owner/Operator’s most recent Cybersecurity Assessment Plan.
 - c. The Owner/Operator must submit the Cybersecurity Assessment Plan report required by subparagraph F.2.e. of this section on an annual basis. The first report must be submitted to TSA no later than 12 months from the date the Owner/Operator *submitted* their first Cybersecurity Assessment Plan as required by this Security Directive. All subsequent annual reports must be submitted to TSA no later than 12 months from the date of TSA’s *approval* of the most recent Cybersecurity Assessment Plan.

IV. RECORDS

- A. *Use of previous plans, assessments, tests, and evaluations.* As applicable, Owner/Operators may use previously developed plans, assessments, tests, and evaluations to meet the requirements of this Security Directive. If the Owner/Operator relies on these materials, they must include an index of the records and their location organized in the same sequence as the requirements in this Security Directive. In addition, these materials must be explicitly incorporated by reference into the Cybersecurity Implementation Plan and made available to TSA upon request.
- B. *Protection of sensitive security information.* The Owner/Operator must, at a minimum, store and transmit the following information required by this Security Directive consistent with the requirements in 49 CFR part 1520:¹²
1. Plans and reports; and
 2. Audit, testing, or assessment results.
- C. *Documentation to Establish Compliance*
1. The Owner/Operator must make records necessary to establish compliance with this Security Directive available to TSA upon request for inspection and/or copying.
 2. TSA may request to inspect or copy the following documents to establish compliance with this Security Directive:
 - a. Hardware/software asset inventory, including supervisory control, and data acquisition systems.
 - b. Firewall rules.
 - c. Network diagrams, switch and router configurations, architecture diagrams, publicly routable internet protocol addresses, and Virtual Local Area Networks.
 - d. Policy, procedural, and other documents that informed the development, and documented implementation of, the Owner/Operator's Cybersecurity Implementation Plan, Cybersecurity Incident Response Plan, Cybersecurity Assessment Program, and assessment or audit results.
 - e. Data providing a "snapshot" of activity on and between Information and Operational Technology systems such as –
 - i. Log files;

¹² Owner/Operators may contact SSI@tsa.dhs.gov for more information on how to comply with requirements for the protection of Sensitive Security Information.

- ii. A capture of network traffic (e.g., packet capture (PCAP)), not to exceed a period of twenty-four hours, as identified and directed by TSA;
 - iii. “East-West Traffic” of Operational Technology systems/sites/environments within the scope of this Security Directive’s requirements; and
 - iv. “North-South Traffic” between Information and Operational Technology systems, and the perimeter boundaries between them.
- f. Any other records or documents necessary to establish compliance with this Security Directive.

V. PROCEDURES FOR SECURITY DIRECTIVES

A. General Procedures

1. *Corfirm Receipt.* Immediately provide written confirmation of receipt of this Security Directive via e-mail to SurfOpsRail-SD@tsa.dhs.gov;
2. *Dissemination.* Immediately disseminate the information and measures in this Security Directive to corporate senior management and security management representatives. The Owner/Operator must provide the applicable security measures in this Security Directive to the Owner/Operator’s direct employees and authorized representatives responsible for implementing applicable security measures as necessary to ensure compliance.

B. *Comments.* Owner/Operators may comment on this Security Directive by submitting data, views, or arguments in writing to TSA via e-mail at TSA-Surface@tsa.dhs.gov. Any comments referring to specific measures in this Security Directive must be protected in accordance with the requirements in 49 CFR part 1520. TSA may amend the Security Directive based on comments received. Submission of a comment does not delay the effective date of the Security Directive or requirement to comply with the provisions of the Security Directive.

C. *Submission of Documentation to TSA:* Owner/Operators are required to submit documents in a manner prescribed by TSA. TSA will provide Owner/Operators specific instructions for submission of required documents.

VI. AMENDMENTS TO CYBERSECURITY IMPLEMENTATION PLAN

- A. *Changes to ownership or control of operations.* An Owner/Operator required to submit a Cybersecurity Implementation Plan under Section II.B. of this Security Directive must submit a request to amend its Cybersecurity Implementation Plan if, after approval, there are any changes to the ownership or control of the operation.
- B. *Changes to conditions affecting security.* An Owner/Operator required to submit a Cybersecurity Implementation Plan under Section II.B. of this Security Directive must submit a request to amend its Cybersecurity Implementation Plan if, after approval, the

AR616

Owner/Operator makes, or intends to make, permanent changes to the policies, procedures, or measures approved by TSA, including, but not limited to changes to address:

1. Determinations that a specific policy, procedure, or measure in the Cybersecurity Implementation Plan is ineffective based on results of the audits and assessments required under Section III.F. of this Security Directive; or
 2. The Owner/Operator has identified or acquired new or additional Critical Cyber Systems or capabilities for meeting the requirements in the Security Directive that have not been previously approved by TSA.
- C. *Permanent change.* For purposes of this section, a “permanent change” is one intended to be in effect for 45 or more days.
- D. *Schedule for requesting amendment.* The Owner/Operator must file the request for an amendment to its Cybersecurity Implementation Plan with TSA no later than 50 days after the permanent change takes effect, unless TSA allows a longer time period.
- E. *TSA approval.*
1. TSA may approve a requested amendment to a Cybersecurity Implementation Plan if TSA determines that it is in the interest of public and transportation security and the proposed amendment provides the level of security required under this Security Directive.
 2. TSA may request additional information from the Owner/Operator before rendering a decision.
- F. *Petition for reconsideration.* No later than 30 days after receiving a denial of an amendment to a Cybersecurity Implementation Plan, the Owner/Operator may file a petition for reconsideration following the procedures set in 49 CFR 1570.119.

VII. DEFINITIONS

In addition to the terms defined in 49 CFR 1500.3 and 1570.3, and the Security Directive 1580-21-01 series and Security Directive 1582-21-01 series, the following terms apply to this Security Directive:

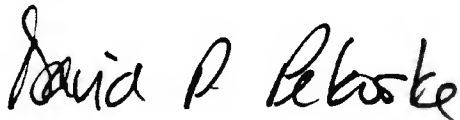
- A. *Authorized Representative* means, for the purpose of this Security Directive, a person who is not a direct employee of the Owner/Operator, but is authorized to act on the Owner/Operator’s behalf to perform measures required by the Security Directive and/or contained within the Owner/Operator’s TSA-approved Cybersecurity Implementation Plan. The term authorized representative may include agents, contractors, and subcontractors. This term does not include Managed Security Service Providers.

- B. ***Business critical functions*** means the Owner/Operator's determination of capacity or capabilities to support functions necessary to meet operational needs and supply chain expectations.
- C. *Component* has the same meaning as "component" as defined in 49 CFR 236.903.
- D. *Critical Cyber System* means any Information or Operational Technology system or data that, if compromised or exploited, could result in operational disruption. Critical Cyber Systems include those business services that, if compromised or exploited, could result in operational disruption.
- E. *Cybersecurity Architecture Design Review* means a technical assessment based on government and industry-recognized standards, guidelines, and best practices that evaluates systems, networks, and security services to determine if they are designed, built, and operated in a reliable and resilient manner. These reviews must be designed to be applicable to the Owner/Operator's Information and Operational Technology systems.
- F. *Cybersecurity incident* means an event that, without lawful authority, jeopardizes, disrupts or otherwise impacts, or is reasonably likely to jeopardize, disrupt or otherwise impact, the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on the system. This definition includes an event that is under investigation or evaluation by the Owner/Operator as a possible cybersecurity incident without final determination of the event's root cause or nature (such as malicious, suspicious, or benign).
- G. *Days* means calendar days unless otherwise indicated. As used for compliance deadlines, if a requirement must be met on a date that is a national holiday, the compliance deadline will be the next federal business day after the holiday.
- H. *East-West traffic* means, in a networking context, the lateral movement of network traffic within a trust zone or local area network.
- I. *Group policy* means a centralized place for administrators to manage and configure operating systems, applications and users' settings that can be used to increase the security of users' computers and help defend against both insider threats and external attacks.
- J. *Information Technology system* means any services, equipment, or interconnected systems or subsystems of equipment that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information that fall within the responsibility of the Owner/Operator to operate and maintain.
- K. *Interdependencies* means relationships of reliance within and among Information and Operational Technology systems that must be maintained for those systems to operate and provide services.

- L. *Managed Security Service Providers* means for the purposes of this Security Directive, a person who is not a direct employee of the Owner/Operator, but who provides one or more services or capabilities that the Owner/Operator is using to perform measures required by the Security Directive and/or contained within the Owner/Operator's TSA-approved Cybersecurity Implementation Plan. Managed Security Service Providers generally provide a logical service or capability. Managed Security Service Providers are not Authorized Representatives.
- M. *Memorized secret authenticator* means a type of authenticator comprised of a character string intended to be memorized by, or memorable to, the subscriber, permitting the subscriber to demonstrate something they know as part of an authentication process.
- N. *North-South traffic* means network traffic that moves through a perimeter boundary into another trust level.
- O. *Operational disruption*, for purposes of this Security Directive, means a deviation from or interruption of business critical functions that results from a compromise or loss of data, system availability, system reliability, or control of systems.
- P. *Operational Technology system* is a general term that encompasses several types of control systems, including industrial control systems, supervisory control and data acquisition systems, distributed control systems, and other control system configurations, such as programmable logic controllers, fire control systems, and physical access control systems, often found in the industrial sector and critical infrastructure. Such systems consist of combinations of programmable electrical, mechanical, hydraulic, pneumatic devices or systems that interact with the physical environment or manage devices that interact with the physical environment.
- Q. *Owner/Operator* means a railroad carrier that operates rolling equipment on track that is part of the general railroad system of transportation.
- R. *Phishing* means tricking individuals into disclosing sensitive personal information through deceptive computer-based means such as internet web sites or e-mails using social engineering or counterfeit identifying information.
- S. *Positive train control (PTC)* has the same meaning as "positive train control" as defined in 49 CFR 236.1003.
- T. *Security, Orchestration, Automation, and Response (SOAR)* means capabilities that enable Owner/Operators to collect inputs monitored by the security operations team. For example, alerts from the security information and event management system and other security technologies – where incident analysis and triage can be performed by leveraging a combination of human and machine power – help define, prioritize and drive standardized incident response activities. These capabilities allow an Owner/Operator to define incident analysis and response procedures in a digital workflow format.
- U. *Shared account* means an account that is used by multiple users with a common authenticator to access systems or data. A shared account is distinct from a group

account, which is a collection of user accounts that allows administrators to group similar user accounts together in order to grant them the same rights and permissions. Group accounts do not have common authenticators.

- V. *Spam* means electronic junk mail or the abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
- W. *Tor*, also known as The Onion Router, means software that allows users to browse the web anonymously by encrypting and routing requests through multiple relay layers or nodes. Tor software obfuscates a user's identity from anyone seeking to monitor online activity (such as nation states, surveillance organizations, information security tools). This deception is possible because the online activity of someone using Tor software appears to originate from the Internet Protocol address of a Tor exit node, as opposed to the address of the user's computer.
- X. *Trust relationship* means an agreed upon relationship between two or more system elements that is governed by criteria for secure interaction, behavior, and outcomes relative to the protection of assets. This term refers to trust relationships between system elements implemented by hardware, firmware, and software.
- Y. *Unauthorized access of an Information Technology or Operational Technology system* means access from an unknown source; access by a third party or former employee; an employee accessing systems for which he or she is not authorized; and may include a non-malicious Owner/Operator policy violation such as the use of a shared credential by an employee otherwise authorized to access it.



David P. Pekoske

Administrator

Transportation Security Administration