No. 13-894

In the Supreme Court of the United States

DEPARTMENT OF HOMELAND SECURITY, PETITIONER

v.

ROBERT J. MACLEAN

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE FEDERAL CIRCUIT

BRIEF FOR PETITIONER

DONALD B. VERRILLI, JR.
Solicitor General
Counsel of Record
STUART F. DELERY
Assistant Attorney General
IAN HEATH GERSHENGORN
Deputy Solicitor General
ERIC J. FEIGIN
Assistant to the Solicitor General
DOUGLAS N. LETTER
H. THOMAS BYRON III
MICHAEL P. GOODMAN
Attorneys

Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

STEVAN E. BUNNELL
General Counsel
U.S. Department of Homeland Security
Washington, D.C. 20528

QUESTION PRESENTED

Congress has directed that the Transportation Security Administration "shall prescribe regulations prohibiting" the "disclosure of information obtained or developed" in carrying out certain transportation-security functions, if the agency "decides" that "disclosing the information would * * * be detrimental" to transportation security. Aviation and Transportation Security Act, Pub. L. No. 107-71, § 101(e), 115 Stat. 603; Homeland Security Act of 2002, Pub. L. No. 107-296, Tit. XVI, § 1601(b), 116 Stat. 2312. Such information is referred to in the regulations as "sensitive security information." See, *e.g.*, 67 Fed. Reg. 8351 (Feb. 22, 2002).

The question presented is whether certain statutory protections codified at 5 U.S.C. 2302(b)(8)(A), which are inapplicable when an employee makes a disclosure "specifically prohibited by law," can bar an agency from taking an enforcement action against an employee who intentionally discloses sensitive security information.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Statutes and regulations:

Statutes and regulations—Continued: Page

Statutes and regulations—Continued: Page

Miscellaneous—Continued: Page

In the Supreme Court of the United States

No. 13-894

DEPARTMENT OF HOMELAND SECURITY, PETITIONER

v.

ROBERT J. MACLEAN

ON WRIT OF CERTIORARI TO
THE UNITED STATES COURT OF APPEALS
FOR THE FEDERAL CIRCUIT

BRIEF FOR PETITIONER

OPINIONS BELOW

The opinion of the court of appeals (Pet. App. 1a-18a) is reported at 714 F.3d 1301. The opinions of the Merit Systems Protection Board (Pet. App. 19a-56a, 113a-139a) are reported at 116 M.S.P.R. 562 and 112 M.S.P.R. 4. The orders of the administrative judges (Pet. App. 57a-112a, 140a-164a) are unreported.

JURISDICTION

The judgment of the court of appeals was entered on April 26, 2013. A petition for rehearing was denied on August 30, 2013 (Pet. App. 165a-166a). On November 19, 2013, the Chief Justice extended the time within which to file a petition for a writ of certiorari to and including December 28, 2013. On December 18, 2013, the Chief Justice further extended the time to and including January 27, 2014, and the petition was filed

on that date. The jurisdiction of this Court rests on 28 U.S.C. 1254(1).

STATUTES AND REGULATIONS INVOLVED

Pertinent statutory and regulatory provisions are set forth in the appendix to this brief. App., *infra*, 1a-27a.

STATEMENT

1. Following the attacks of September 11, 2001, Congress enacted the Aviation and Transportation Security Act (ATSA), Pub. L. No. 107-71, 115 Stat. 597, to "address the security of the nation's transportation system." H.R. Conf. Rep. No. 296, 107th Cong., 1st Sess. 54 (2001). In enacting the ATSA, Congress determined that "the best way to ensure effective Federal management of the nation's transportation system is through the creation of a new Administration" within the Department of Transportation "to be called the Transportation Security Administration (TSA)," whose responsibilities would "encompass security in all modes of transportation." *Id.* at 55; see ATSA, § 101(a), 115 Stat. 597 (49 U.S.C. 114(a)). The TSA's duties under the ATSA include daily security screening for air travel; receipt, analysis, and distribution of intelligence relating to transportation security; improvement of existing security procedures; assessment of security measures for cargo transportation; and oversight of security at airports and other transportation facilities. § 101(a), 115 Stat. 597-598 (49 U.S.C. 114(d)(1)-(2), (e)(1), (f)(1)-(3), (6)-(8) and (10)-(11)).

In addition to creating the TSA and specifying its responsibilities, the ATSA also ensured that certain information acquired or developed in the course of security activities, the dissemination of which could be

harmful, would be shielded from public disclosure. A preexisting statute, 49 U.S.C. 40119(b) (2000), had instructed that, "[n]otwithstanding" the Freedom of Information Act (FOIA), 5 U.S.C. 552, the Federal Aviation Administration was required to "prescribe regulations prohibiting disclosure of information obtained or developed in carrying out security or research and development activities under" certain security-related provisions of Title 49, if it determined that "disclosing the information would * * * be an unwarranted invasion of personal privacy," "reveal a trade secret or privileged or confidential commercial or financial information," or "be detrimental to the safety of passengers in air transportation." See Act of July 5, 1994, Pub. L. No. 103-272, 108 Stat. 1117; see also Air Transportation Security Act of 1974, Pub. L. No. 93-366, § 316, 88 Stat. 417. Pursuant to that congressional mandate, the Federal Aviation Administration had promulgated detailed regulations designating certain information as "sensitive security information" (SSI) and restricting the disclosure of such information. See, *e.g.*, 14 C.F.R. Pt. 191 (2000); see also 14 C.F.R. Pt. 191 (1977). The ATSA reassigned the duty to promulgate those regulations to the TSA, § 101(e), 115 Stat. 603, and the SSI regulations (with certain amendments) were subsequently transferred over to the TSA's authority, see 67 Fed. Reg. 8351 (Feb. 22, 2002).

The Homeland Security Act of 2002 (HSA), Pub. L. No. 107-296, Tit. IV, Subtit. A, § 403(2), 116 Stat. 2178, moved the TSA into the newly created Department of Homeland Security. A separate provision of that Act, currently codified at 49 U.S.C. 114(r), expanded upon the TSA's statutory mandate to prohibit the disclosure

of sensitive information. See HSA, Tit. XVI, § 1601(b), 116 Stat. 2312; see also Consolidated Appropriations Act, 2008, Pub. L. No. 110-161, Tit. V, § 568, 121 Stat. 2092 (moving former Section 114(s) to Section 114(r)). Section 114(r)(1) provides:

> Notwithstanding section 552 of title 5, the Under Secretary shall prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of the Aviation and Transportation Security Act (Public Law 107-71) or under chapter 449 of this title if the Under Secretary decides that disclosing the information would—
>
> (A) be an unwarranted invasion of personal privacy;
>
> (B) reveal a trade secret or privileged or confidential commercial or financial information; or
>
> (C) be detrimental to the security of transportation.

49 U.S.C. 114(r)(1). Congress also amended 49 U.S.C. 40119(b) to impose substantially similar obligations on the Secretary of Transportation. HSA, Tit. XVI, § 1601(a), 116 Stat. 2312.

In 2003, when the events giving rise to this case occurred, the TSA's SSI regulations generally defined SSI to include a range of sensitive information, including security plans, threat-detection mechanisms, and vulnerability assessments. In particular, the regulations defined SSI to include, *inter alia*, "[s]pecific details of aviation security measures * * * includ[ing] * * * information concerning specific numbers of Federal Air Marshals, deployments or

missions, and the methods involved in such operations," as well as other information deemed essential to transportation security, such as "[a]ny approved, accepted, or standard security program" adopted under certain regulations; "Security Directives and Information Circulars" promulgated under certain regulations; "[a]ny selection criteria used in any security screening process, including for persons, baggage, or cargo"; "[a]ny security contingency plan or information and any comments, instructions, or implementing guidance pertaining thereto"; and the technical specifications of certain security equipment (such as screening equipment). 49 C.F.R. 1520.7(a)-(f) and (j) (2002); see 67 Fed. Reg. at 8340. The regulations generally prohibited the disclosure of SSI unless the recipient had a "need to know" the information, 49 C.F.R. 1520.5(a) (2002); specifically defined the circumstances in which an individual had such a "need to know," see 49 C.F.R. 1520.5(b) (2002); and stated that an unauthorized disclosure was "grounds for a civil penalty and other enforcement or corrective action." 49 C.F.R. 1520.17; see 49 C.F.R. 1520.5(d) (2002).

The TSA's current SSI regulations, as well as the SSI regulations separately promulgated by the Department of Transportation, are substantially similar to the 2003 version (but include some new categories of SSI that have been added over the last decade). See 49 C.F.R. 1520.5, 1520.9(a)(2), 1520.17 (TSA); see also 49 C.F.R. Pt. 15 (Department of Transportation). A significant amount of information that the TSA designates as SSI would qualify to be classified under the President's Article II national-security powers. The TSA designates it as SSI, rather than formally classifying it, in order that it can, if necessary, be

shared quickly and securely with non-government personnel (such as airport and airline employees) whose cooperation is critical to ensuring transportation security, but who may not be cleared for more sensitive classified information. See, *e.g.*, 70 Fed. Reg. 1380 (Jan. 7, 2005) (stating that an "original intent" of the SSI regulations was "to share vulnerability assessments and threat information with entities in all transportation modes that need the information to help forestall future attacks").

2. Respondent is a former federal air marshal who was hired by the TSA in 2001. Pet. App. 2a. Under the air-marshal program as established by the ATSA, the TSA deploys federal air marshals on passenger flights in order to protect those flights from hijacking and other in-flight dangers. 49 U.S.C. 44917(a)(1)-(2); see ATSA, § 105(a), 115 Stat. 606. The TSA has discretionary authority to deploy federal air marshals on any flight, and it is required to station a federal air marshal on any flight that, in the agency's judgment, "present[s] high security risks." 49 U.S.C. 44917(a)(1)-(2); see ATSA, § 105(a), 115 Stat. 606-607.

As previously noted, the TSA has, since the inception of its SSI regulations, designated information about air-marshal deployments as SSI. See 67 Fed. Reg. at 8352; 49 C.F.R. 1520.7(j) (2002) (defining SSI to include "information concerning specific numbers of Federal Air Marshals, deployments or missions"); 49 C.F.R. 1520.5(b)(8)(ii) (defining SSI to include "[i]nformation concerning the deployments, numbers, and operations of * * * Federal Air Marshals, to the extent it is not classified national security information"). During his employment as an air marshal, respondent received written notification of the agen-

cy's SSI policies (and signed a statement acknowledging that he read and understood them), and he underwent in-person SSI training as well. Pet. App. 51a, 73a. He has testified that it was "very, very clear that you did not tell flight numbers and times of the flights you flew missions on" and that he was aware of other air marshals who had been terminated for disclosing such information. *Id.* at 73a-74a (citation omitted); see *ibid.* (noting respondent's awareness that air marshals had been fired for disclosing their flight information to significant others meeting them at the airport). Respondent also testified that "[i]f I told somebody that a particular flight was *not* going to have any protection on it, that endangered that specific flight." *Id.* at 74a (emphasis added; citation omitted).

In July 2003, the TSA briefed respondent on a "potential plot" to hijack United States airliners, Pet. App. 20a (citation omitted), in which the "[a]ttack venues [might] include the United Kingdom, Italy, Australia, or the East coast of the United States," J.A. 16. Shortly thereafter, respondent received a text message from the TSA stating that, for a particular window of time, the TSA would not be deploying federal air marshals on overnight missions from Las Vegas. Pet. App. 2a; *id.* at 20a & n.1. Respondent's supervisor subsequently explained to him that the TSA lacked sufficient funds for those particular missions. *Id.* at 59a. Respondent informed both his supervisor and the Office of the Inspector General for the Department of Homeland Security of his personal view that the TSA's decision about how to deploy its air marshals was not in the best interests of public safety. *Id.* at 21a. He was not, however, satisfied with the responses he received. *Ibid.*

Respondent then decided to reveal the TSA's air-marshal-deployment plans to the news media, in an effort to "create a controversy" that would force the TSA to change those plans. Pet. App. 2a (citation omitted). Respondent has testified that it did not matter to him, in formulating that scheme, whether the information he planned to reveal was SSI, *id.* at 81a, and an administrative judge found his claim that he was unaware the information was SSI not to be credible, *id.* at 81a, 100a-103a. After respondent told an MSNBC reporter about the TSA's deployment plans, the reporter published an article exposing those plans to the public and criticizing them. *Id.* at 2a. Members of Congress also criticized the plans. *Ibid.* The TSA ultimately did not follow the course of action that had been outlined in the original text message. *Ibid.*

The TSA was not aware initially that respondent had been the source of the disclosure. Pet. App. 2a. It learned of his involvement, however, when respondent appeared on NBC Nightly News to discuss a separate matter, in a disguise that proved to be inadequate. *Ibid.* The TSA removed respondent from his position as a federal air marshal for disclosing SSI without authorization. *Id.* at 2a-3a. The deciding official later testified that by divulging "information on * * * a particular group of flights that were not covered" by federal air marshals, respondent had "created a vulnerability within the aviation system" and "set us up for a possible another [sic] 9/11 incident." *Id.* at 91a (emphasis omitted).

3. Respondent challenged his removal before the Merit Systems Protection Board (MSPB), "an independent Government agency that operates like a

court" and has jurisdiction to review certain personnel actions. 5 C.F.R. 1200.1; see, *e.g.*, 5 U.S.C. 7513(d). One of respondent's claims was that his removal had violated 5 U.S.C. 2302(b)(8)(A). Pet. App. 3a. Under Section 2302(b)(8)(A), an agency generally cannot "take * * * a personnel action" against an employee for disclosing certain types of information, when the employee "reasonably believe[d]" that the information showed a "violation of any law, rule, or regulation" or "gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety." 5 U.S.C. 2302(b)(8)(A)(i) and (ii).[1] Section 2302(b)(8)(A) does not apply, however, if the employee's disclosure was "specifically prohibited by law." 5 U.S.C. 2302(b)(8)(A).

The MSPB ultimately rejected respondent's Section 2302(b)(8)(A) argument and sustained the agency's decision to remove him. Pet. App. 19a-56a. The MSPB recognized that the TSA, pursuant to a legislative mandate to prescribe regulations preventing the disclosure of certain types of information, had promulgated regulations that "identified SSI subject to * * * statutory nondisclosure as including information relating to [federal-air-marshal] deployments."

---

[1] The current version of Section 2302(b)(8)(A)(i) differs slightly from the version in effect at the time of respondent's disclosure. Compare 5 U.S.C. 2302(b)(8)(A)(i) ("*any* violation of any law, rule, or regulation") (emphasis added), with 5 U.S.C. 2302(b)(8)(A)(i) (2006) ("*a* violation of any law, rule, or regulation") (emphasis added). Because that amendment is not relevant to the question presented, this brief will cite the current version.

Id. at 33a.[2] The MSPB additionally observed that the Ninth Circuit, in a separate proceeding that respondent had initiated, had "unequivocally declared that the information disclosed by [respondent] constituted SSI as defined in those regulations." *Id.* at 34a; see *MacLean* v. *Department of Homeland Sec.*, 543 F.3d 1145, 1150 (2008) (per curiam); 49 C.F.R. 1520.7(j) (2002). The MSPB accordingly reasoned that because respondent had "disclosed information that is specifically prohibited from disclosure by a regulation promulgated pursuant to an express legislative directive from Congress to TSA," the "disclosure was 'specifically prohibited by law'" for purposes of Section 2302(b)(8)(A). Pet. App. 34a-35a.

4. The Federal Circuit vacated the MSPB's decision and remanded for further proceedings. Pet. App. 1a-18a; see 5 U.S.C. 7703(a)(1) and (b)(1) (2006) (authorizing an employee to seek Federal Circuit review of an adverse MSPB decision). The court of appeals recognized that respondent's removal had reflected a proper application of the TSA's regulations. Pet. App. 5a-7a. It also agreed with the government that removal had been a reasonable penalty for a disclosure that had "compromised flight safety," created a

---

[2] In the MSPB's view, the relevant legislative mandate was the version of 49 U.S.C. 40119(b) that was in effect when the TSA initially promulgated the regulations. Pet. App. 33a n.9. The briefs and decisions below accordingly focused on Section 40119(b). However, at the time of respondent's disclosure, the statute requiring and authorizing the TSA's SSI regulations was actually the provision now codified at 49 U.S.C. 114(r). See pp. 3-5, *supra*. For that reason, and for the sake of simplicity, this brief will focus on Section 114(r). In any event, because the language of the two statutes is nearly identical, the legal analysis would be similar under either one.

"threat to public safety," and "could have had catastrophic consequences." *Id.* at 7a-9a. The court concluded, however, that respondent's disclosure of SSI had not been "specifically prohibited by law" and that he was therefore entitled to invoke the protections of Section 2302(b)(8)(A). *Id.* at 10a-17a.

The court of appeals initially stated that it believed the parties to be in agreement that the "'specifically prohibited by law' proviso" applies only to disclosures "prohibited by a statute" and not to disclosures prohibited "by a regulation." Pet. App. 12a; see *id.* at 13a (perceiving the parties to agree that "a regulation * * * cannot be 'law'"). The court subsequently acknowledged, however, that "[r]egulations promulgated pursuant to Congress's express instructions *would* qualify as specific legal prohibitions" for purposes of applying the proviso. *Id.* at 15a (emphasis added). And it viewed the legislative mandate to promulgate SSI regulations to present "a very close case," because the mandate included a direct "charge" to the agency "to prescribe regulations pursuant to specific criteria (i.e., only information that would be detrimental to transportation safety)." *Ibid.* But the court ultimately concluded that, because the statute "gives some discretion to the Agency to fashion regulations for prohibiting disclosure," the statute's criteria were too "general" to "'specifically prohibit' employee conduct." *Id.* at 14a. In reaching that conclusion, the court relied in part on language from a Senate Report, without acknowledging that the report had addressed an unenacted version of Section 2302(b)(8), which had contained the phrase "prohibited by statute" rather than the phrase "specifically prohibited by law." *Id.* at 13a-14a (citing S. Rep. No.

969, 95th Cong., 2d Sess. 21 (1978) (Senate Report)); see Senate Report 154.

Having decided the critical legal question, the court of appeals remanded the case for a determination of whether respondent had reasonably believed his disclosure evidenced "a substantial and specific danger to public health or safety" or one of the other subjects listed in Section 2302(b)(8)(A). Pet. App. 16a. Judge Wallach concurred to express the view that "the facts alleged, if proven, allege conduct at the core of" the activity protected by that provision. *Id.* at 18a. The court of appeals denied the government's petition for rehearing en banc. *Id.* at 165a-166a.

SUMMARY OF ARGUMENT

The Federal Circuit recognized that Congress has directed the TSA to prescribe regulations prohibiting disclosures deemed "detrimental" to transportation security. Pet. App. 11a (citation omitted); see 49 U.S.C. 114(r)(1)(C). It also recognized that regulations implementing that congressional directive expressly designated information about federal-air-marshal deployments as SSI and that respondent's disclosure of such deployment information was accordingly forbidden. Pet. App. 5a-7a; see 49 C.F.R. 1520.7(j) (2002). The Federal Circuit nevertheless held that respondent's disclosure was not "specifically prohibited by law." 5 U.S.C. 2302(b)(8)(A); see Pet. App. 10a-17a. That holding precludes disciplinary action against respondent or any other federal employee for public disclosures of SSI that expose vulnerabilities in transportation security, so long as the disclosure was motivated by "reasonabl[e]"—even if unmeritorious—disagreement with the government's decision to give higher priority to other security con-

cerns. 5 U.S.C. 2302(b)(8)(A). The Federal Circuit's decision is wrong, dangerous, and warrants reversal.

A. The legislatively created scheme that prohibited respondent's disclosure constituted a "specific[] prohibit[ion] by law" for purposes of Section 2302(b)(8)(A). First, the SSI regulations that explicitly barred the disclosure of "information concerning specific numbers of Federal Air Marshals, deployments or missions," 49 C.F.R. 1520.7(j) (2002), in themselves triggered the "specifically prohibited by law" proviso. In the absence of a "clear showing" of contrary congressional intent, the phrase "by law" is presumed to include both statutes and substantive regulations that have the force and effect of law. *Chrysler Corp.* v. *Brown*, 441 U.S. 281, 295-296 (1979). The nondisclosure regulations at issue here not only had the force and effect of law, but were affirmatively required by Congress, which was already aware of the content of those regulations when it enacted Section 114(r)(1).

Neither the Federal Circuit nor respondent has set forth any "clear showing" that Congress intended these congressionally dictated nondisclosure regulations to fall outside the scope of the phrase "by law." Although the text and legislative history of Section 2302(b)(8)(A) contain some indication that Congress did not want agencies to invoke internal procedural regulations to silence whistleblowers, any such concern would not extend to nondisclosure regulations promulgated pursuant to Congress's own explicit command. Respondent's narrow view of the "specifically prohibited by law" proviso to include only Acts of Congress, and not their direct implementing regulations, would impermissibly revive a rejected version of

the proviso that would have used the term "by statute" rather than the term "by law."

Second, even if the term "by law" were interpreted to refer solely to restrictions imposed by statutes, respondent's disclosure was "specifically prohibited by law" under Section 114(r)(1) itself. In *Administrator, FAA* v. *Robertson*, 422 U.S. 255 (1975), this Court construed the statutory phrase "specifically exempted from disclosure by statute" to encompass a statute that authorized an agency to exercise broad interest-balancing discretion to determine whether certain information should be disclosed. The Section 2302(b)(8)(A) proviso at issue here ("specifically prohibited by law") is at least as broad as the one at issue in *Robertson*, and the degree of agency discretion under Section 114(r)(1) to prohibit the disclosure of information is, if anything, narrower than the degree of agency discretion at issue in *Robertson*. The applicability of the Section 2302(b)(8)(A) proviso in the circumstances of this case thus follows *a fortiori* from *Robertson*.

Respondent and the Federal Circuit have avoided the conclusion that Section 114(r)(1) satisfies the "specifically prohibited by law" proviso only by looking to the legislative history of a proposed version of the Section 2302(b)(8)(A) proviso that Congress never enacted. Although a Senate Report favored a more limited version of the proviso, Congress ultimately adopted proviso language broader than the language proposed in the Senate Report. In any event, even the narrow version of the proviso discussed in the Senate Report would have encompassed any statute that "establishes particular criteria for withholding or refers to particular types of matters to be withheld,"

Senate Report 21, a category that includes Section 114(r)(1). In fact, Section 114(r)(1) is much more specifically prohibitory than another statute—which simply provided that "the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure," 50 U.S.C. 403(d)(3) (1976)—that the Senate Report identified as falling within its version of the proviso. Senate Report 21-22.

B. The Federal Circuit's decision gives short shrift to Congress's express intent both to prohibit disclosure of SSI and to handle concerns about confidential matters internally without exposing sensitive information to public view. In crafting Section 2302(b)(8), Congress balanced its desire to encourage reports of perceived government missteps with the need to protect the secrecy of information whose disclosure could cause serious harm. Section 2302(b)(8) does not authorize a federal employee to go to the media *whenever* he has a reasonable belief that particular information shows government misfeasance. Instead, when that information has been designated confidential (because its publication would, for example, constitute an unwarranted invasion of privacy or be detrimental to transportation security), the employee receives statutory protection only if he raises his concerns to the agency's Inspector General, to the Office of Special Counsel, or to other appropriate officials, who can investigate thoroughly while keeping the information secure. 5 U.S.C. 2302(b)(8)(B). He can be disciplined, however, if he eschews those avenues and instead chooses to reveal that information to the public, 5 U.S.C. 2302(b)(8)(A).

The decision below imperils public safety by dramatically reducing the effectiveness of Congress's scheme for keeping sensitive security information from falling into the wrong hands. SSI by its nature involves public-safety matters. Its content frequently reflects difficult choices about how best to allocate finite security resources; those difficult choices will often be subject to plausible objections; and employees will thus frequently have a basis for claiming to "reasonably believe[]," 5 U.S.C. 2302(b)(8), that disclosing SSI will be beneficial. But as Congress recognized in enacting Section 114(r)(1), public disclosure of information designated as SSI—which includes, for example, security plans, threat-detection mechanisms, and vulnerability assessments—could have disastrous consequences. Congress could not have intended that a single employee's objection to a TSA decision, no matter how well-intentioned that objection might be, would allow the employee to take matters into his own hands and divulge information that could be exploited to jeopardize the country's transportation infrastructure and the lives and livelihoods of those who depend upon it.

ARGUMENT

THE DISCLOSURE OF SENSITIVE SECURITY INFORMATION IS "SPECIFICALLY PROHIBITED BY LAW" WITHIN THE MEANING OF 5 U.S.C. 2302(b)(8)(A)

The Federal Circuit's decision disregards the plain text of Section 2302(b)(8)(A), seriously undermines the effectiveness of the congressionally mandated SSI regime, invites individual federal employees to make disclosures that will threaten public safety, and should be reversed. In the course of its efforts to secure the Nation's transportation network, the TSA necessarily

develops and acquires a great deal of information, including information about security vulnerabilities, that has the potential to cause extreme harm if publicly disclosed. In recognition of that fact, Congress has directed that the TSA "shall prescribe regulations" prohibiting disclosures that would, in the expert judgment of the TSA, "be detrimental to the security of transportation." 49 U.S.C. 114(r)(1)(C).

The decision below, however, effectively permits individual federal employees to override the TSA's judgments about the dangers of public disclosure. According to the court of appeals, no matter how harmful it might be for particular SSI to fall into the wrong hands, an employee is not subject to discipline for publicizing that SSI, so long as he reasonably believes that the disclosure serves one of the interests listed in 5 U.S.C. 2302(b)(8)(A). The Federal Circuit's decision thus clears a path for any of TSA's more than 60,000 employees with access to SSI to do what respondent did here: go public with an internal disagreement about how best to allocate finite security resources; put lives in danger by identifying potential vulnerabilities in areas that have received fewer resources; and then attempt to avoid repercussions on the ground that he reasonably believed that publicizing such vulnerabilities revealed "a substantial and specific danger to public health or safety," 5 U.S.C. 2302(b)(8)(A)(ii).

That result contravenes the manifest intent of Congress. The protections afforded by Section 2302(b)(8)(A) do not apply to public disclosures that are "specifically prohibited by law." That proviso squarely encompasses public disclosures of SSI, which are prohibited pursuant to an express congressional

directive. Employees with concerns that implicate SSI are instead protected by Section 2302(b)(8)(B), which covers disclosures of confidential information to intragovernmental oversight authorities that are able to investigate possible problems without the need for harmful public disclosures.

A. Section 2302(b)(8)(A)'s "Specifically Prohibited By Law" Proviso Encompasses The Congressionally Created SSI Nondisclosure Scheme

The Federal Circuit's conclusion that the disclosure of SSI is not "specifically prohibited by law" is flawed as a matter of both statutory interpretation and common sense. The SSI regulations reflect an expert agency's implementation of Congress's express instruction that disclosures dangerous to transportation security be prohibited. See 49 U.S.C. 114(r)(1)(C); 67 Fed. Reg. at 8351; 49 C.F.R. Pt. 1520. Whether the relevant "law" is considered to be the regulations that Congress required the TSA to promulgate, the statute that directed the agency to promulgate those regulations, or the two in combination, the bottom line is that the very purpose of the SSI scheme designed by Congress is to "specifically prohibit[]" the exposure of information the secrecy of which is vital to public safety.

1. The term "by law" in Section 2302(b)(8)(A) includes legislatively mandated SSI regulations

The SSI regulations on their face "specifically prohibited" respondent's public disclosure that certain flights from Las Vegas (those requiring overnight missions) would not have air marshals aboard. See Pet. App. 5a-7a (concluding that respondent violated a nondisclosure prohibition); *MacLean* v. *Department of*

Homeland Sec., 543 F.3d 1145, 1150 (9th Cir. 2008) (per curiam) (same). At the time respondent made that disclosure, those regulations expressly prohibited sharing "information concerning specific numbers of Federal Air Marshals, deployments or missions, and the methods involved in such operations" with unauthorized persons. 49 C.F.R. 1520.7(j) (2002); see 49 C.F.R. 1520.5(a)-(b) (2002); see also 49 C.F.R. 1520.5(d) (2002). And the prohibition against respondent's disclosure was a prohibition "by law" whether it appeared directly in the statute or instead in the regulations that the statute required the TSA to promulgate.[3]

a. In *Chrysler Corp.* v. *Brown*, 441 U.S. 281 (1979), this Court construed the statutory phrase "authorized by law" in 18 U.S.C. 1905 (1976) to include not just authorization conferred directly by statute, but also by "properly promulgated, substantive agency regulations." 441 U.S. at 295. The Court observed that "[i]t has been established in a variety of contexts that properly promulgated, substantive agency regulations have the 'force and effect of law.'" *Ibid.*; see *id.* at 295 n.18 (citing cases). "This doctrine," the Court continued, "is so well established that agency regulations implementing federal statutes have been held to pre-

[3] Respondent has contended (Br. in Opp. 14-18) that the government waived this argument in the court of appeals. For reasons explained in the government's certiorari-stage filings (Pet. 15-16; Cert. Reply Br. 10-12), that contention is incorrect. In any event, the Court presumably considered this argument at the certiorari stage and concluded that it did not present an impediment to effective review of the question presented. See *Verizon Commc'ns Inc.* v. *FCC*, 535 U.S. 467, 530-531 (2002); *United States* v. *Williams*, 504 U.S. 36, 40-41 (1992); *Stevens* v. *Department of the Treasury*, 500 U.S. 1, 8 (1991).

empt state law under the Supremacy Clause." *Id.* at 295-296. "It would therefore take a clear showing of contrary legislative intent before the phrase 'authorized by law' in § 1905 could be held to have a narrower ambit than the traditional understanding." *Id.* at 296.

As respondent appears to acknowledge, that same "clear showing" rule should apply to Section 2302(b)(8)(A)'s "specifically prohibited by law" proviso. See Br. in Opp. 23 (recognizing that "the word 'law' sometimes—perhaps even usually—encompasses regulations" and referencing *Chrysler Corp.*'s "clear showing" rule). The "well established" interpretive principles discussed in *Chrysler Corp.*, and which the Court in *Chrysler Corp.* applied to a decades-old statute, were just as "well established" six months before *Chrysler Corp.* was decided, when Congress enacted Section 2302(b)(8)(A) proviso as part of the Civil Service Reform Act of 1978 (CSRA), Pub. L. No. 95-454, § 101(a), 92 Stat. 1116. Indeed, consistent with *Chrysler Corp.*, standard definitions of "law" around that time would naturally have encompassed regulations of the sort described in that decision. See, *e.g.*, *American Heritage Dictionary of the English Language* 741 (1976) (defining "law" to include "[t]he body of rules governing the affairs of man within a community"); *Black's Law Dictionary* 1028 (rev. 4th ed. 1968) (defining law to include "[t]hat which is laid down, ordained, or established"); *Webster's New International Dictionary* 1401 (2d ed. 1958) (defining "law" in the context of law and political science primarily to include "[a] rule of (external) conduct or action which is prescribed, or is formally recognized as binding, by the supreme governing authority and is enforced by a sanction, as any edict, decree, rescript,

order, ordinance, statute, resolution, rule, judicial decision, usage, etc., made, or recognized, and enforced, by the controlling authority" or "[t]he whole body of such rules").

b. Nothing in Section 2302(b)(8)(A) provides a "clear showing," *Chrysler Corp.*, 441 U.S. at 296, that the phrase "by law" excludes substantive nondisclosure regulations, like the SSI regulations, that were promulgated pursuant to an express congressional directive. Such regulations are inextricably intertwined with the statutes that mandate their promulgation and are "law" to the same extent that the statutes themselves are.

The Court's decision in *Chrysler Corp.* explains that a regulation has the "force and effect of law" when it "affect[s] individual rights and obligations," 441 U.S. at 302 (citation omitted); its "promulgation * * * conform[s] with any procedural requirements imposed by Congress," *id.* at 303; and the statute authorizing it can "reasonably" be said to have "contemplate[d]" the regulation, *id.* at 308. The SSI regulations satisfy all three requirements. First, they "certainly affect individual rights and obligations," because they address issues of "confidentiality" and the disclosure of information. *Id.* at 303. Second, the procedural soundness of the regulations has not been disputed in this case.[4] Third, a congressional "grant of

---

[4] In its initial adoption, in 2002, of an amended version of the Federal Aviation Administration's preexisting SSI regulations, the TSA followed the procedure specified in 5 U.S.C. 553(b)(B), which allows an agency to promulgate a final rule without prior notice-and-comment "when the agency for good cause finds (and incorporates the finding and a brief statement of reasons therefor in the rules issued) that notice and public procedure thereon are imprac-

authority" cannot more clearly "contemplate[] the regulations issued," *id.* at 308, than in a circumstance, like this one, where Congress has specifically directed an agency to issue such regulations. Indeed, the connection in this case is particularly strong, given that the TSA, pursuant to the ATSA, had *already* promulgated SSI regulations—including the regulation designating air-marshal-deployment information as SSI—when Congress enacted Section 114(r). See HSA, § 1601(b), 116 Stat. 2312; 67 Fed. Reg. at 8340-8341, 8352. Section 114(r)'s renewal, and expansion, of the TSA's obligation to promulgate nondisclosure regulations is most reasonably interpreted to reflect Congress's approval of the regulations already in place. Cf. *Lorillard* v. *Pons*, 434 U.S. 575, 580 (1978) ("Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change.").

Respondent contends, however, (Br. in Opp. 19-20) that Section 2302(b)(8)(A)'s "specifically prohibited by law" proviso cannot encompass *any* regulations, regardless of how explicitly Congress may have required their promulgation, because other places in the statute include the phrase "law, rule, or regulation." That contention is unsound. The juxtaposition of the

---

ticable, unnecessary, or contrary to the public interest." *Ibid.*; see 67 Fed. Reg. at 8340. The TSA explained that the rulemaking "mostly [was] an administrative action moving rules from one title to another in the Code of Federal Regulations"; that the ATSA "impose[d] a statutory mandate" for certain amendments to the regulations; and that the agency had determined that "notice and public comment under 5 U.S.C. 553(b) are impracticable and contrary to the public interest." *Id.* at 8349. The final rule solicited comments for future revisions. *Id.* at 8340, 8349.

term "law" with the phrase "law, rule, or regulation" may sometimes support an inference that the term "law" alone is to *some* degree narrower in scope than the phrase "law, rule, or regulation." As the Court explained in *Department of the Treasury* v. *Federal Labor Relations Authority*, 494 U.S. 922 (1990), a "statute that in one section refers to 'law, rule or regulation,' and in another section to only 'laws' cannot, unless we abandon all pretense at precise communication, be deemed to mean the same thing in both places." *Id.* at 932; see *Russello* v. *United States*, 464 U.S. 16, 23 (1983). But the fact that "law" may be narrower than "law, rule, or regulation" does not mean that "by law" should have the particular, especially cramped, meaning advanced by respondent, under which *no* regulation—not even one Congress has mandated—counts as "law."

As the Court recognized in *Department of the Treasury* v. *Federal Labor Relations Authority*, it would be "a permissible (though not an inevitable) construction" to conclude that "the term 'applicable laws' * * * extends to *some*, but not all, rules and regulations," notwithstanding its appearance in a statute that also referred to "'any law, rule or regulation.'" 494 U.S. at 932-933 (emphasis added; citation omitted). Similarly here, Congress's use of the expansive phrase "law, rule, or regulation" does not in itself suggest that the definitions of "law," "rule," and "regulation" are mutually exclusive. Many, if not all, "regulations" can also be considered "rules," and vice versa. *Black's Law Dictionary* 1451 (rev. 4th ed. 1968) (defining "regulation" to include "a *rule* or order prescribed for management or government") (emphasis added); *id.* at 1496 (defining "rule" to include "[a]n

established standard, guide, or *regulation*") (emphasis added). And it is hardly unusual for a "rule" or a "regulation" to be considered "law." See *Chrysler Corp.*, 441 U.S. at 295-296. Accordingly, Congress could readily have employed the catch-all phrase "law, rule, or regulation" in certain places in an effort to capture the entirety of all three categories, without intending that the categories be considered completely distinct. The broader phrase might, for example, encompass procedural rules and regulations that, under *Chrysler Corp.*, would not meet the definition of "law" standing alone.

In the particular context of Section 2302(b)(8)(A), an interpretation of "by law" that encompasses at least some regulations—including, at a minimum, nondisclosure regulations that Congress has required a federal agency to adopt—is far more coherent than respondent's alternative. If, as respondent suggests, the term "by law" excludes all regulations, then even if Congress enacted a statute directing the TSA to "promulgate a regulation barring the disclosure of air-marshal-deployment information," and the TSA complied with that statute, no "law" would prohibit the disclosure of such information for purposes of Section 2302(b)(8)(A). That conclusion defies both language and logic. Whether the text of a statute itself bars disclosure, or instead expressly directs an agency to promulgate a regulation to that effect, the end result (a prohibition on disclosure) is the product of congressional design, and it makes no sense to view the result as accomplished "by law" in one case but not the other.

Contrary to respondent's contention (Br. in Opp. 20), his crabbed interpretation of the phrase "by law"

finds no support in the "broader structure" of Section 2302(b)(8)(A). Respondent notes (*ibid.*) that Section 2302(b)(8)(A)'s protections are inapplicable both when a disclosure was "specifically prohibited by law" and when the disclosed information was "specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs." He reasons from this that Congress did not intend for courts to create other "unmentioned" exceptions. *Ibid.* (citation omitted). The issue here, however, is not the existence of an "unmentioned" exception, but instead the scope of the *express* exception for disclosures "specifically prohibited by law."

Respondent also suggests (Br. in Opp. 20) that the exception for certain Executive Orders "suggests intentional exclusion" of other "categor[ies] of Executive branch authority." But unlike substantive regulations that an agency is specifically required by statute to promulgate, an Executive Order that lacks a clear statutory basis would not necessarily fall within the presumptive definition of "law." See *Chrysler Corp.*, 441 U.S. at 304-308 (suggesting that regulations authorized solely by Executive Order would not be considered "law" in the context of 18 U.S.C. 1905 (1976)). Congress's clarification of how Section 2302(b)(8)(A) applies in the context of Executive Orders accordingly creates no inference that congressionally mandated SSI regulations fail to qualify as "law."

c. The legislative history of Section 2302(b)(8)(A) is consistent with an interpretation of the "specifically prohibited by law" proviso as including the SSI regulations that Section 114(r)(1) directed the TSA to promulgate. When Congress was designing the CSRA, the Senate proposed a version of the proviso

that would have been limited to only those disclosures "prohibited by *statute*." Senate Report 21, 154 (emphasis added). Congress did not, however, adopt that proposal, but instead enacted a more broadly worded proviso, applicable to disclosures "specifically prohibited by *law*." 5 U.S.C. 2302(b)(8)(A) (emphasis added); see H.R. Conf. Rep. No. 1717, 95th Cong., 2d. Sess. 130 (1978) (Conference Report). Congress's replacement of the word "statute" with the word "law" indicates that Congress did *not* intend the proviso to be limited solely to statutes. See *Russello*, 464 U.S. at 23-24 ("Where Congress includes limiting language in an earlier version of a bill but deletes it prior to enactment, it may be presumed that the limitation was not intended.").

The legislative history does support the view that Congress intended to exclude *some* regulations from the scope of the proviso. As respondent notes, an early proposal by the House included a proviso for disclosures "prohibited by law, rule, or regulation." Br. in Opp. 21; see Senate Report 21. The final language of the proviso as enacted falls somewhere in between that early House proposal and the subsequent Senate proposal to "narrow[] the proviso" to cover only statutes, Senate Report 21. The conference report accompanying the final version stated that the proviso "does not refer to agency rules and regulations" but instead "to statutory law and court interpretations of those statutes." Conference Report 130. The enacted language of the proviso thus appears to reflect, to a degree, the concerns that had animated the Senate proposal. Those concerns, however, do not provide a "clear showing," *Chrysler Corp.*, 441 U.S. at

296, that Congress intended the term "law" to be equivalent to the discarded term "statute."

The Senate's concerns had been directed to the possibility that agencies might adopt "*internal procedural* regulations against disclosure" that would "discourage an employee from coming forward with allegations of wrongdoing." Senate Report 21 (emphasis added). During a mark-up session, Senator Humphrey had noted that "it is standard procedure for agencies to have internal regulations specif[ying] which agency employ[ee]s can talk to the press," and expressed concern with proviso language under which "all non-specified employees could be denied the whistle blower protection." Senate Comm. on Governmental Affairs, *Mark-Up Session on S. 2640: The Civil Service Reform Act of 1978*, at 15 (May 22, 1978). He deemed such a prospect to be inconsistent with the proviso's basic purpose "to protect against disclosure of classified information or other information that most of us agree should be kept secret," and he accordingly advocated calibrating the proviso's language to ensure that "information that should be kept secret will continue to be without unnecessarily restricting the whistle blower protection." *Id.* at 15-16; see *id.* at 8-9 (suggestion by Senator Javits to narrow the proviso to avoid "enabl[ing] an agency to suffocate a whistle blower").

The Senate's concerns with "internal procedural" regulations, like the press-related regulations mentioned by Senator Humphrey, would not apply to nondisclosure regulations, like the SSI regulations at issue here, that Congress *itself* expressly instructed an agency to promulgate. The latter set of regulations are a subclass of "substantive rules," which both Con-

gress and this Court have long recognized to be distinct from "rules of agency organization, *procedure*, or practice." *Chrysler Corp.*, 441 U.S. at 301 (emphasis added) (quoting 5 U.S.C. 553(b) and (d) (1976)). They reflect the requirements of a specific congressional nondisclosure statute; they "implement th[at] statute," *id.* at 302-303 (citation omitted); and they are therefore comfortably encompassed within the text of the "specifically prohibited by law" proviso as enacted by Congress.

2. Section 114(r)(1) itself "specifically prohibit[s]" the disclosure of SSI

Even if the relevant inquiry were restricted to the four corners of an Act of Congress, the disclosure in this case would still have been "specifically prohibited by law" within the meaning of Section 2302(b)(8)(A). Section 114(r) sets forth three "specific[]" categories of information: information whose disclosure, in the TSA's judgment, would "be an unwarranted invasion of personal privacy"; information whose disclosure, in the TSA's judgment, would "reveal a trade secret or privileged or confidential commercial or financial information"; and information whose disclosure would, in the TSA's judgment, "be detrimental to the security of transportation." 49 U.S.C. 114(r)(1)(A)-(C). And Section 114(r)(1) "prohibit[s]" the disclosure of that information by providing that the TSA "shall prescribe regulations" to that effect. 49 U.S.C. 114(r)(1).

a. The applicability of the "specifically prohibited by law" proviso in the circumstances of this case follows *a fortiori* from this Court's decision in *Administrator, FAA* v. *Robertson*, 422 U.S. 255 (1975). That case involved a provision of the FOIA, known as Exemption 3, which at that time permitted an agency to

withhold from the public any information "specifically exempted from disclosure by statute." *Id.* at 257 (quoting 5 U.S.C. 552(b)(3) (1970)). The issue in *Robertson* was whether particular information was "specifically exempted from disclosure by statute," within the meaning of Exemption 3, when an agency had exercised discretion conferred by statute to designate that information as confidential. *Id.* at 256-258 & n.4. The statute in question permitted the agency to withhold a certain type of information from disclosure whenever the agency had made a "judgment" that disclosure was "not required in the interest of the public" and "would adversely affect the interests" of someone objecting to the disclosure. *Id.* at 258 n.4 (quoting 49 U.S.C. 1504 (1970)). This Court concluded that information withheld in that fashion was covered by Exemption 3, *id.* at 261-267, rejecting the view that the scheme vested too much discretion in the agency to satisfy Exemption 3's "specifically exempted from disclosure by statute" proviso, see *id.* at 260, 267.

As a textual matter, the result in *Robertson* directly controls this case. The proviso at issue here ("specifically prohibited by law") is effectively identical in all relevant respects to the proviso at issue in *Robertson* ("specifically exempted from disclosure by statute"). The only relevant difference between the two provisos—Section 2302(b)(8)(A)'s use of the term "law," rather than "statute"—suggests that the proviso here is *broader* than the proviso at issue in *Robertson*. At the same time, the statutory authority at issue here (to promulgate regulations precluding the disclosure of information deemed "detrimental to the security of transportation") is, if anything, even *more* specifically prohibitory than the statutory authority at

issue in *Robertson* (to preclude the disclosure of information based on an agency's balancing of public and private interests). The Federal Circuit's view (Pet. App. 14a) that the statutory authority at issue in this case "does not 'specifically prohibit'" disclosures, because it "provides only general criteria for withholding information and gives some discretion to the Agency," accordingly cannot be squared with *Robertson*. The combination of a broader proviso and a more specific nondisclosure statute makes this an even easier case for proviso coverage than *Robertson* itself.

Respondent, echoing the Federal Circuit, asserts that Section 114(r)(1) "'does not expressly prohibit employee disclosures' at all; it 'only empowers the Agency to prescribe regulations prohibiting disclosure.'" Br. in Opp. 24 (quoting Pet. App. 13a). But Section 114(r)(1) is just as prohibitory as the statute at issue in *Robertson*. Both statutes anticipate and rely on agency action—in *Robertson*, adjudication; here, regulation—to carry out congressional intent. This case also presents the additional circumstance, not present in *Robertson*, that Congress was actually on notice, when it enacted Section 114(r)(1), of precisely how the agency would implement that statute. As previously noted, Congress enacted Section 114(r)(1) against a backdrop that already included SSI regulations promulgated by the TSA, including the regulation that respondent violated here, and its reauthorization of such regulations presumably reflects its approval of preexisting agency practice. See p. 22, *supra*.

Respondent, again echoing the Federal Circuit, also asserts that Section 114(r)(1) is insufficiently specific because "[a]t best, it 'provides only general crite-

ria for withholding information.'" Br. in Opp. 25 (quoting Pet. App. 14a). But the Court in *Robertson* did not require the statute at issue in that case "to specify or categorize the particular documents it authorizes to be withheld" in order to fall within Exemption 3's "'specifically exempted from disclosure by statute'" proviso, 422 U.S. at 260; see *id.* at 265. And there is no sound basis for finding the enumerated criteria in Section 114(r)(1) to be any *less* specific than the more amorphous interest-balancing contemplated by the statute in *Robertson*.

b. Although much of the specific reasoning in *Robertson* turned on factors tied to FOIA, see 422 U.S. at 261-267, *Robertson*'s interpretation of the then-existing text of the Exemption 3 proviso is instructive on the meaning of Section 2302(b)(8)(A)'s proviso. Congress enacted Section 2302(b)(8)(A) just three years after *Robertson*. This Court has "often observed that when 'judicial interpretations have settled the meaning of an existing statutory provision, repetition of the same language in a new statute indicates, as a general matter, the intent to incorporate its . . . judicial interpretations as well.'" *Jerman* v. *Carlisle, McNellie, Rini, Kramer & Ulrich, L.P.A.*, 559 U.S. 573, 589-590 (2010) (quoting *Bragdon* v. *Abbott*, 524 U.S. 624, 645 (1998)); see, *e.g.*, *Merrill Lynch, Pierce, Fenner & Smith Inc.* v. *Dabit*, 547 U.S. 71, 85-86 (2006). Congress thus presumably expected that courts would interpret the Section 2302(b)(8)(A) proviso at least as broadly as this Court had interpreted the similar Exemption 3 proviso at issue in *Robertson*.

Evidence of Congress's reaction to *Robertson* supports that presumption. In the wake of *Robertson*, Congress narrowed the language of FOIA's Exemp-

tion 3 to apply only to information "specifically exempted from disclosure by statute (other than section 552b of this title), *provided that* such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld." 5 U.S.C. 552(b)(3) (1976) (emphasis added); see *Consumer Prod. Safety Comm'n* v. *GTE Sylvania, Inc.*, 447 U.S. 102, 121 n.18 (1980). But when Congress enacted Section 2302(b)(8)(A) shortly thereafter, it included a "specifically prohibited by law" proviso that was not subject to any similar limitations. CSRA, § 101(a), 92 Stat. 1116. The natural inference is that Congress did not intend to incorporate those limitations, and instead intended the Section 2302(b)(8)(A) proviso to be interpreted in a broader fashion, consistent with *Robertson*.

That inference is reinforced by the legislative history of Section 2302(b)(8)(A). As previously discussed, the Senate had proposed a version of the proviso that would have applied only to disclosures "prohibited by statute." Senate Report 154. The Senate Report accompanying that proposal expressed the view that the suggested "prohibited by statute" proviso should encompass only the types of statutes covered by the amended Exemption 3. *Id.* at 21. But Congress rejected the Senate's proposal in favor of a more broadly worded proviso ("specifically prohibited by law"). 5 U.S.C. 2302(b)(8)(A); see H.R. Rep. No. 1403, 95th Cong., 2d Sess. 146 (1978); Conference Report 130. Even if adoption of the Senate version would have implied the existence of the various nontextual limita-

tions to which the Senate Report referred, rejection of the Senate version implies the opposite.

3. In any event, assuming *arguendo* that the Section 2302(b)(8)(A) proviso did incorporate those implicit limitations—as respondent and the Federal Circuit have assumed, see Br. in Opp. 24; Pet. App. 13a-14a—the legislative mandate to promulgate the SSI regulations would satisfy them. Even under the Senate Report's restrictive view, "a statute which establishes particular criteria for withholding or refers to particular types of matters to be withheld" would fall within the proviso's scope. Senate Report 21. The legislative mandate here, which describes specific categories of information that the TSA is required to keep confidential, see 49 U.S.C. 114(r)(1), "establishes particular criteria for withholding or refers to particular types of matters to be withheld."

Section 114(r)(1) compares favorably in this respect with a statute that the Senate Report specifically identified as one that would fall within the narrow proviso that it proposed. The Senate Report, in the course of setting forth its view that a "prohibited by statute" proviso would implicitly incorporate limitations like those in FOIA's amended Exemption 3, expressed its "understanding that section 102(d)(3) of the National Security Act of 1947 * * * has been held to be" a statute that would satisfy those limitations. *Id.* at 21-22. Section 102(d)(3) provided that "the Director of Central Intelligence shall be responsible for protecting intelligence sources and methods from unauthorized disclosure." 50 U.S.C. 403(d)(3) (1976). The legislative mandate here—which expressly directs the TSA to prohibit the disclosure of three particular categories of information in a particular

manner (promulgation of regulations), see 49 U.S.C. 114(r)(1)—is even more specific and prohibitory than Section 102(d)(3). And not only the Senate Report, but also this Court, has understood Section 102(d)(3) to be covered by FOIA's amended Exemption 3. Senate Report 21-22; *CIA* v. *Sims*, 471 U.S. 159, 167-168 (1985) (agreeing with the "uniform view among other federal courts" that Section 102(d)(3) is "a withholding statute under Exemption 3"). There is no sound reason why Section 102(d)(3) would fall within FOIA's Exemption 3, but Section 114(r)(1) would fall outside the more broadly worded Section 2302(b)(8)(A) proviso.[5]

B. Allowing Federal Employees To Publicly Disclose SSI Would Subvert Congress's Intent And Create Serious Risks To Public Safety

The Federal Circuit's conclusion in this case, that Section 2302(b)(8)(A) can immunize respondent from disciplinary action for disclosing SSI, undermines the careful line that Congress drew between concerns that

---

[5] As respondent appears to recognize (Br. in Opp. 6-8, 30), Section 114(r)'s preamble, which clarifies that the TSA shall promulgate nondisclosure regulations "[n]otwithstanding section 552 of title 5," 49 U.S.C. 114(r)(1), does not limit the effect of those regulations to the context of FOIA requests, but instead is consistent with the promulgation of regulations that prohibit unauthorized disclosures more generally. See Pet. App. 5a-9a; *MacLean*, 543 F.3d at 1149-1150. Were it otherwise, TSA employees could make sensitive and dangerous disclosures at will, so long as they were not responding to a FOIA request when doing so. See *Public Citizen, Inc.* v. *FAA*, 988 F.2d 186, 195 (D.C. Cir. 1993) ("Congress can hardly have intended for the FAA to be able to resist under [a predecessor to Section 114(r)(1)] a FOIA request for security-sensitive information * * * but not a request for precisely the same information under another statute.").

an employee may voice in public and those that he should instead raise with the Inspector General or the Office of Special Counsel. The general purpose of Section 2302(b)(8) is to "encourage government personnel to blow the whistle on wasteful, corrupt or illegal government practices without fearing retaliatory action by their supervisors or those harmed by the disclosures." *Marano* v. *Department of Justice*, 2 F.3d 1137, 1142 (Fed. Cir. 1993). But Congress did not pursue that objective to the exclusion of all others. The statute also embodies a countervailing concern that employees not reveal to the public—and instead reveal only to internal watchdogs—information that has legitimately been shielded from public view for reasons unrelated to whistleblowing.

1. Under Section 2302(b)(8), any employee who comes across information that he "reasonably believes" shows a "violation of any law, rule, or regulation" or "gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety" can raise his concerns without fear of employment-related reprisal. 5 U.S.C. 2302(b)(8)(A)(i) and (ii), (B)(i) and (ii). But the manner in which he may raise those concerns depends upon whether the disclosure of information is "specifically prohibited by law" (or "specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs"). 5 U.S.C. 2302(b)(8)(A). If no such prohibition exists, then there is no reason to believe that any harm from public disclosure will be significant enough to outweigh the benefits of public debate, and the employee may go public with the information. See *ibid.*

If such a prohibition does exist, however, Section 2302(b)(8) does not permit the employee himself to decide whether the benefits of public disclosure outweigh the interests underlying the prohibition against it. Instead, the employee, if he wishes to avoid disciplinary action, must raise his concerns through internal channels: he may go either "to the Inspector General of [the] agency or another employee designated by the head of the agency to receive such disclosures" or "to the Special Counsel," who operates independently of the agency. 5 U.S.C. 2302(b)(8)(B);[6] see 5 U.S.C. 1211-1212. Those channels provide meaningful opportunities for the exposure of problems within an agency that warrant corrective action, while at the same time respecting the need to shield particular information from public view. If, for example, the employee goes to the Special Counsel, the Special Counsel is required to evaluate the information within 15 days, 5 U.S.C. 1213(b); may compel the agency to investigate the matter and file a written report, 5 U.S.C. 1213(c)-(d); and must transmit the report (generally along with any comments from the employee whose disclosure initiated the investigation) to the President, relevant congressional committees, and, potentially, other agencies (such as the Department of Justice), 5 U.S.C. 1213(e); see 5 U.S.C. 1213(h) (generally requiring the Special Counsel to maintain the originating employee's confidentiality).

---

[6] As with Section 2302(b)(8)(A)(i), see note 1, *supra*, the text of Section 2302(b)(8)(B)(i) differs slightly from the version in effect at the time of respondent's disclosure. Compare 5 U.S.C. 2302(b)(8)(B)(i), with 5 U.S.C. 2302(b)(8)(B)(i) (2006). That amendment is not relevant here.

Under the Federal Circuit's decision, however, an employee may disregard those carefully designed procedures for maintaining the confidentiality of sensitive information and unilaterally choose to make public disclosures that the TSA has legitimately determined, in response to a congressional directive, to "be detrimental to the security of transportation." 49 U.S.C. 114(r)(1)(C). Congress could not have intended the confidentiality of sensitive security information to depend so precariously on the idiosynchratic individual judgments of each of the TSA's more than 60,000 employees. Congress presumably understood, in crafting Section 2302(b)(8), that not every internal complaint would be resolved to the complaining employee's complete satisfaction. Respondent's individual experience in this case (which apparently did not include any attempt to contact the Office of Special Counsel) did not entitle him to substitute his own judgment for that of Congress, decide that sensitive matters are better debated in public, and divulge information whose confidentiality is critical to transportation security.

Once respondent publicly exposed a set of flights that would not be protected by air marshals, he left the TSA with no choice but to put air marshals on at least some of those flights, regardless of whether doing so would otherwise have been the optimal plan. See Pet. App. 93a-94a. Although respondent and his supporters—including, perhaps, some individual Members of Congress—might believe that respondent's disclosure in this case was beneficial, the "specifically prohibited by law" proviso does not allow for a post hoc inquiry into whether the ends justified the means. The proviso instead forecloses employees

from arrogating to themselves the authority to make individual choices with such far-reaching and potentially injurious effects. However benign a particular employee's motives might be, he will most likely lack access to all of the information that led the TSA to make particular security decisions; his "reasonabl[e] belie[f]" in the salutary effect of his disclosure will not necessarily be correct; and Section 2302(b)(8)(A) does not invest him with veto authority over the agency's normal decisionmaking processes on sensitive security matters.

2. Permitting an employee who discloses SSI to invoke Section 2302(b)(8)(A) as a defense to a resulting employment action would embolden federal employees to disclose SSI and gravely endanger public safety. Information designated as SSI includes "[s]ecurity programs and contingency plans"; "[s]ecurity [d]irectives"; specifications of security equipment and procedures; "[v]ulnerability assessments"; methods used to detect threats; operational and technical details of particular security measures; security screening procedures; "[s]ecurity training materials"; "[i]dentifying information of certain transportation security personnel"; and lists of systems and assets "the incapacity or destruction of [which] would have a debilitating impact on transportation security." 49 C.F.R. 1520.5(b)(1)-(2), (4)-(5) and (7)-(12) (emphases omitted). Any of that information, if improperly disclosed, could present a serious threat to the security of the Nation's transportation network and put lives at risk.

Armed with such information, someone might, for example, gain the ability to circumvent existing security measures, evade existing threat-detection procedures, or pinpoint specific vulnerabilities in the na-

tional transportation infrastructure. As the Federal Circuit recognized, respondent's own disclosure of flights that would not be protected by federal air marshals "compromised flight safety," created a "threat to public safety," and "could have had catastrophic consequences." Pet. App. 8a. Even information that might not appear on its face to expose a security vulnerability (say, the fact that a particular federal air marshal will be on a particular flight) could potentially be exploited to create one (say, by interfering with the air marshal's ability to make the flight). It will not always be possible for the TSA to modify its plans in time to mitigate the disclosed vulnerability. Even when it is possible to do so, the effort may "force[] the Agency to reallocate scarce resources," *ibid.*, thereby diminishing the resources available in areas that the agency initially determined to present greter risks to public safety. And a disclosure of information about screening technology (such as the calibration of metal detectors), for example, would require major investments of time, resources, and infrastructure improvements to remedy; could take months, if not years, to complete; and would require considerable expenditure of federal funds.

The Federal Circuit attempted to downplay the impact of its decision by pointing out that the government may still "discipline employees who reveal SSI for personal gain or due to negligence, or who disclose information that the employee does not reasonably believe evidences a substantial and specific danger to public health or safety." Pet. App. 16a-17a. But that is cold comfort. SSI, by its very nature, concerns security matters. Employees will thus frequently be able to claim that they are publicly disclosing SSI in

an effort to expose flaws in transportation security. Many of those employees may later be deemed by the MSPB, or a court, to have had a "reasonabl[e] belie[f]" that the disclosure "evidences * * * a substantial and specific danger to public health or safety," 5 U.S.C. 2302(b)(8)(A)(ii), or another type of "reasonabl[e] belie[f]" that qualifies for protection under Section 2302(b)(8)(A). Even if some employees' disclosures are not ultimately deemed to be within the scope of Section 2302(b)(8)(A), the increased likelihood of that result will itself erode the SSI scheme's deterrent effect and encourage more disclosures, which are immediately harmful whether or not the responsible employee is eventually subject to disciplinary action.

3. Respondent's suggestion (Br. in Opp. 32) that the TSA is "try[ing] to circumvent whistleblower protections through regulation" is seriously misguided. The prohibition on public disclosure of air-marshal-deployment information has an obvious, legitimate, and compelling security rationale entirely unrelated to any potential desire by the agency to "conceal wrongdoing," *id.* at 31 (citation omitted). As the MSPB concluded, Pet. App. 50a-54a, and the Federal Circuit agreed, *id.* at 7a-9a, it was reasonable for the TSA to remove respondent for his dangerous disclosure of such information, even assuming his subjective motive for doing so was benign. See *id.* at 52a-53a (MSPB's determination that respondent's actions "could have created a significant security risk" and that he "did not exhibit the good judgment that the agency can legitimately expect of its law enforcement personnel"). If the Federal Circuit's decision is allowed to stand, however, the MSPB may well conclude

(as the concurring judge in the court of appeals apparently would, see *id.* at 18a) that the TSA must reinstate respondent to a position where he will again have access to SSI.

To the extent any concern exists that the TSA might apply Section 114(r) in an overbroad manner calculated to deter legitimate disclosures, Congress can address—and has, in fact, addressed—that concern. In 2009, Congress amended Section 114(r) to clarify that "[n]othing in this subsection, or any other provision of law, shall be construed to authorize the designation of information as sensitive security information" in order to "conceal a violation of law, inefficiency, or administrative error"; "prevent embarrassment to a person, organization, or agency"; "restrain competition"; or "prevent or delay the release of information that does not require protection in the interest of transportation security, including basic scientific research information not clearly related to transportation security." 49 U.S.C. 114(r)(4)(A)-(D); see American Communities' Right to Public Information Act, Pub. L. No. 111-83, § 561(c)(1), 123 Stat. 2182; see also 49 U.S.C. 40119(b) (similar limitations on the Department of Transportation's authority). Although that amendment postdates the disclosures at issue here, the regulation that prohibited respondent's disclosure of air-marshal-deployment information clearly was not enacted for any of those now-impermissible purposes. There is no doubt that such information "require[s] protection in the interest of transportation security," and the Federal Circuit agreed with the government that respondent's specific disclosure jeopardized flight safety. 49 U.S.C. 114(r)(4)(D); see Pet. App. 7a-9a. Respondent's seri-

ous breach of security protocol accordingly should not be immunized under Section 2302(b)(8)(A).

CONCLUSION

The judgment of the court of appeals should be reversed.

Respectfully submitted.

DONALD B. VERRILLI, JR.
Solicitor General
STUART F. DELERY
Assistant Attorney General
IAN HEATH GERSHENGORN
Deputy Solicitor General
ERIC J. FEIGIN
Assistant to the Solicitor General
DOUGLAS N. LETTER
H. THOMAS BYRON III
MICHAEL P. GOODMAN
Attorneys

STEVAN E. BUNNELL
General Counsel
U.S. Department of Homeland Security

JULY 2014

APPENDIX

1. 5 U.S.C. 2302 provides in pertinent part:

Prohibited personnel practices

* * * * *

(b) Any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority—

* * * * *

(8) take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment because of—

(A) any disclosure of information by an employee or applicant which the employee or applicant reasonably believes evidences—

(i) any violation of any law, rule, or regulation, or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety,

if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs; or

(B) any disclosure to the Special Counsel, or to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures, of information which the employee or applicant reasonably believes evidences—

(i) any violation (other than a violation of this section) of any law, rule, or regulation, or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

* * * * *

2. 5 U.S.C. 2302 (2006) provided in pertinent part:

Prohibited personnel practices

* * * * *

(b) Any employee who has authority to take, direct others to take, recommend, or approve any personnel action, shall not, with respect to such authority—

* * * * *

(8) take or fail to take, or threaten to take or fail to take, a personnel action with respect to any employee or applicant for employment because of—

(A) any disclosure of information by an employee or applicant which the employee or applicant reasonably believes evidences—

(i) a violation of any law, rule, or regulation, or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety,

if such disclosure is not specifically prohibited by law and if such information is not specifically required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs; or

(B) any disclosure to the Special Counsel, or to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures, of information which the employee or applicant reasonably believes evidences—

(i) a violation of any law, rule, or regulation, or

(ii) gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety;

* * * * *

3. 49 U.S.C. 114(r) provides in pertinent part:

Transportation Security Administration

* * * * *

(r) NONDISCLOSURE OF SECURITY ACTIVITIES.—

(1) IN GENERAL.—Notwithstanding section 552 of title 5, the Under Secretary shall prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of the Aviation and Transportation Security Act (Public Law 107-71) or under chapter 449 of this title if the Under Secretary decides that disclosing the information would—

(A) be an unwarranted invasion of personal privacy;

(B) reveal a trade secret or privileged or confidential commercial or financial information; or

(C) be detrimental to the security of transportation.

(2) AVAILABILITY OF INFORMATION TO CONGRESS.—Paragraph (1) does not authorize information to be withheld from a committee of Congress authorized to have the information.

(3) LIMITATION ON TRANSFERABILITY OF DUTIES.—Except as otherwise provided by law, the Under Secretary may not transfer a duty or power under this subsection to another department, agency, or instrumentality of the United States.

(4) LIMITATIONS.—Nothing in this subsection, or any other provision of law, shall be construed to authorize the designation of information as sensitive security information (as defined in section 1520.5 of title 49, Code of Federal Regulations)—

(A) to conceal a violation of law, inefficiency, or administrative error;

(B) to prevent embarrassment to a person, organization, or agency;

(C) to restrain competition; or

(D) to prevent or delay the release of information that does not require protection in the interest of transportation security, including basic scientific research information not clearly related to transportation security.

4. 49 U.S.C. 114(s) (2000 & Supp. II 2002) provided in pertinent part:

Transportation Security Administration

* * * * *

(s) NONDISCLOSURE OF SECURITY ACTIVITIES.—

(1) IN GENERAL.—Notwithstanding section 552 of title 5, the Under Secretary shall prescribe regulations prohibiting the disclosure of information obtained or developed in carrying out security under authority of the Aviation and Transportation Security Act (Public Law 107-71) or under chapter

449 of this title if the Under Secretary decides that disclosing the information would—

(A) be an unwarranted invasion of personal privacy;

(B) reveal a trade secret or privileged or confidential commercial or financial information; or

(C) be detrimental to the security of transportation.

(2) AVAILABILITY OF INFORMATION TO CONGRESS.—Paragraph (1) does not authorize information to be withheld from a committee of Congress authorized to have the information.

(3) LIMITATION ON TRANSFERABILITY OF DUTIES.—Except as otherwise provided by law, the Under Secretary may not transfer a duty or power under this subsection to another department, agency, or instrumentality of the United States.

5. 49 U.S.C. 40119(b) provides in pertinent part:

Security and research and development activities

* * * * *

(b) DISCLOSURE.—(1) Notwithstanding section 552 of title 5 and the establishment of a Department of Homeland Security, the Secretary of Transportation shall prescribe regulations prohibiting disclosure of information obtained or developed in ensuring security

under this title if the Secretary of Transportation decides disclosing the information would—

(A) be an unwarranted invasion of personal privacy;

(B) reveal a trade secret or privileged or confidential commercial or financial information; or

(C) be detrimental to transportation safety.

(2) Paragraph (1) of this subsection does not authorize information to be withheld from a committee of Congress authorized to have the information.

6. 49 U.S.C. 40119(b) (2000 & Supp. I 2001) provided in pertinent part:

Security and research and development activities

* * * * *

(b) DISCLOSURE.—(1) Notwithstanding section 552 of title 5, the Under Secretary shall prescribe regulations prohibiting disclosure of information obtained or developed in carrying out security or research and development activities under section 44501(a) or (c), 44502(a)(1) or (3), (b), or (c), 44504, 44505, 44507, 44508, 44511, 44512, 44513, 44901, 44903(a), (b), (c), or (e), 44905, 44912, 44935, 44936, or 44938(a) or (b) of this title if the Under Secretary decides disclosing the information would—

(A) be an unwarranted invasion of personal privacy;

(B) reveal a trade secret or privileged or confidential commercial or financial information; or

(C) be detrimental to the safety of passengers in transportation.

(2) Paragraph (1) of this subsection does not authorize information to be withheld from a committee of Congress authorized to have the information.

7. 49 U.S.C. 40119(b) (2000) provided in pertinent part:

Security and research and development activities

* * * * *

(b) DISCLOSURE.—(1) Notwithstanding section 552 of title 5, the Administrator shall prescribe regulations prohibiting disclosure of information obtained or developed in carrying out security or research and development activities under section 44501(a) or (c), 44502(a)(1) or (3), (b), or (c), 44504, 44505, 44507, 44508, 44511, 44512, 44513, 44901, 44903(a), (b), (c), or (e), 44905, 44912, 44935, 44936, or 44938(a) or (b) of this title if the Administrator decides disclosing the information would—

(A) be an unwarranted invasion of personal privacy;

(B) reveal a trade secret or privileged or confidential commercial or financial information; or

(C) be detrimental to the safety of passengers in air transportation.

(2) Paragraph (1) of this subsection does not authorize information to be withheld from a committee of Congress authorized to have the information.

8. 49 C.F.R. 1520 provides in pertinent part:

PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

* * * * *

§ 1520.5 Sensitive security information.

(a) *In general.* In accordance with 49 U.S.C. 114(s), SSI is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would—

(1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person; or

(3) Be detrimental to the security of transportation.

(b) *Information constituting SSI.* Except as otherwise provided in writing by TSA in the interest of public safety or in furtherance of transportation secu-

rity, the following information, and records containing such information, constitute SSI:

(1) *Security programs and contingency plans.* Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including any comments, instructions, or implementing guidance, including—

(i) Any aircraft operator, airport operator, fixed base operator, or air cargo security program, or security contingency plan under this chapter;

(ii) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

(iii) Any national or area security plan prepared under 46 U.S.C. 70103; and

(iv) Any security incident response plan established under 46 U.S.C. 70104.

(2) *Security Directives.* Any Security Directive or order—

(i) Issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, or other authority;

(ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 *et seq.* related to maritime security; or

(iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) *Information Circulars.* Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any—

(i) Information circular issued by TSA under 49 CFR 1542.303, 1544.305, 1548.19, or other authority; and

(ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) *Performance specifications.* Any performance specification and any description of a test object or test procedure, for—

(i) Any device used by the Federal Government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any person, and any weapon, explosive, incendiary, or destructive device, item, or substance; and

(ii) Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.

(5) *Vulnerability assessments.* Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

(6) *Security inspection or investigative information.* (i) Details of any security inspection or investigation of an alleged violation of aviation, maritime, or rail transportation security requirements of Federal

law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(ii) In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

(7) *Threat information.* Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.

(8) *Security measures.* Specific details of aviation, maritime, or rail transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including—

(i) Security measures or protocols recommended by the Federal government;

(ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and

(iii) Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator.

(iv) Any armed security officer procedures issued by TSA under 49 CFR part 1562.

(9) *Security screening information.* The following information regarding security screening under aviation or maritime transportation security requirements of Federal law:

(i) Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person.

(ii) Information and sources of information used by a passenger or property screening program or system, including an automated screening system.

(iii) Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI.

(iv) Any security screener test and scores of such tests.

(v) Performance or testing data from security equipment or screening systems.

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

(10) *Security training materials.* Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out aviation, maritime, or rail transportation security measures required or recommended by DHS or DOT.

(11) *Identifying information of certain transportation security personnel.* (i) Lists of the names or other identifying information that identify persons as—

(A) Having unescorted access to a secure area of an airport, a rail secure area, or a secure or restricted area of a maritime facility, port area, or vessel;

(B) Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport;

(C) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection;

(D) Holding a position as a Federal Air Marshal; or

(ii) The name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.

(12) *Critical aviation, maritime, or rail infrastructure asset information.* Any list identifying systems or assets, whether physical or virtual, so vital to the aviation, maritime, or rail transportation system (including rail hazardous materials shippers and rail hazardous materials receivers) that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is—

(i) Prepared by DHS or DOT; or

(ii) Prepared by a State or local government agency and submitted by the agency to DHS or DOT.

(13) *Systems security information.* Any information involving the security of operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as

critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) *Confidential business information.* (i) Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising therefrom, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures;

(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.

(15) *Research and development.* Information obtained or developed in the conduct of research related to aviation, maritime, or rail transportation security activities, where such research is approved, accepted, funded, recommended, or directed by DHS or DOT, including research results.

(16) *Other information.* Any information not otherwise described in this section that TSA deter-

mines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, TSA or the Secretary of DOT may designate as SSI information not otherwise described in this section.

(c) *Loss of SSI designation.* TSA or the Coast Guard may determine in writing that information or records described in paragraph (b) of this section do not constitute SSI because they no longer meet the criteria set forth in paragraph (a) of this section.

* * * * *

§ 1520.9 Restrictions on the disclosure of SSI.

(a) *Duty to protect information.* A covered person must—

(1) Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it a secure container, such as a locked desk or file cabinet or in a locked room.

(2) Disclose, or otherwise provide access to, SSI only to covered persons who have a need to know, unless otherwise authorized in writing by TSA, the Coast Guard, or the Secretary of DOT.

(3) Refer requests by other persons for SSI to TSA or the applicable component or agency within DOT or DHS.

(4) Mark SSI as specified in § 1520.13.

(5) Dispose of SSI as specified in § 1520.19.

(b) *Unmarked SSI.* If a covered person receives a record containing SSI that is not marked as specified in § 1520.13, the covered person must—

(1) Mark the record as specified in § 1520.13; and

(2) Inform the sender of the record that the record must be marked as specified in § 1520.13.

(c) *Duty to report unauthorized disclosure.* When a covered person becomes aware that SSI has been released to unauthorized persons, the covered person must promptly inform TSA or the applicable DOT or DHS component or agency.

(d) *Additional Requirements for Critical Infrastructure Information.* In the case of information that is both SSI and has been designated as critical infrastructure information under section 214 of the Homeland Security Act, any covered person who is a Federal employee in possession of such information must comply with the disclosure restrictions and other requirements applicable to such information under section 214 and any implementing regulations.

§ 1520.11 Persons with a need to know.

(a) *In general.* A person has a need to know SSI in each of the following circumstances:

(1) When the person requires access to specific SSI to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(2) When the person is in training to carry out transportation security activities approved, accepted, funded, recommended, or directed by DHS or DOT.

(3) When the information is necessary for the person to supervise or otherwise manage individuals carrying out transportation security activities approved, accepted, funded, recommended, or directed by the DHS or DOT.

(4) When the person needs the information to provide technical or legal advice to a covered person regarding transportation security requirements of Federal law.

(5) When the person needs the information to represent a covered person in connection with any judicial or administrative proceeding regarding those requirements.

(b) *Federal, State, local, or tribal government employees, contractors, and grantees.* (1) A Federal, State, local, or tribal government employee has a need to know SSI if access to the information is necessary for performance of the employee's official duties, on behalf or in defense of the interests of the Federal, State, local, or tribal government.

(2) A person acting in the performance of a contract with or grant from a Federal, State, local, or tribal government agency has a need to know SSI if access to the information is necessary to performance of the contract or grant.

(c) *Background check.* TSA or Coast Guard may make an individual's access to the SSI contingent upon satisfactory completion of a security background check or other procedures and requirements for safeguarding SSI that are satisfactory to TSA or the Coast Guard.

(d) *Need to know further limited by the DHS or DOT.* For some specific SSI, DHS or DOT may make a finding that only specific persons or classes of persons have a need to know.

* * * * *

§ 1520.17 Consequences of unauthorized disclosure of SSI.

Violation of this part is grounds for a civil penalty and other enforcement or corrective action by DHS, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

* * * * *

9. 49 C.F.R. 1520 (2002) provided in pertinent part:

PART 1520—PROTECTION OF SENSITIVE SECURITY INFORMATION

* * * * *

§ 1520.5 Records and information protected by others.

(a) *Duty to protect information.* The following persons must restrict disclosure of and access to sensitive security information described in § 1520.7 (a) through (g), (j), (k), and (m) through (r), and, as applicable, § 1520.7 (l) to persons with a need to know and must refer requests by other persons for such information to TSA or the applicable DOT administration:

(1) Each person employed by, contracted to, or acting for a person listed in this paragraph (a).

(2) Each airport operator under part 1542 of this chapter.

(3) Each aircraft operator under part 1544 of this chapter.

(4) Each foreign air carrier under part 1546 of this chapter.

(5) Each indirect air carrier under part 1548 of this chapter.

(6) Each aircraft operator under § 1550.5 of this chapter.

(7) Each person receiving information under § 1520.3 (d).

(8) Each person for which a vulnerability assessment has been authorized, approved, or funded by DOT, irrespective of the mode of transportation.

(b) *Need to know.* For some specific sensitive security information, the Under Secretary may make a finding that only specific persons or classes of persons have a need to know. Otherwise, a person has a need to know sensitive security information in each of the following circumstances:

(1) When the person needs the information to carry out DOT-approved, accepted, or directed security duties.

(2) When the person is in training to carry out DOT-approved, accepted, or directed security duties.

(3) When the information is necessary for the person to supervise or otherwise manage the individuals carrying to carry out DOT-approved, accepted, or directed security duties.

(4) When the person needs the information to advise the persons listed in paragraph (a) of this section regarding any DOT security-related requirements.

(5) When the person needs the information to represent the persons listed in paragraph (a) of this section in connection with any judicial or administrative proceeding regarding those requirements.

(c) *Release of sensitive security information.* When sensitive security information is released to unauthorized persons, any person listed in paragraph

(a) of this section or individual with knowledge of the release, must inform DOT.

(d) *Violation.* Violation of this section is grounds for a civil penalty and other enforcement or corrective action by DOT.

(e) *Applicants.* Wherever this part refers to an aircraft operator, airport operator, foreign air carrier, or indirect air carrier, those terms also include applicants for such authority.

(f) *Trainees.* An individual who is in training for a position is considered to be employed by, contracted to, or acting for persons listed in paragraph (a) of this section, regardless of whether that individual is currently receiving a wage or salary or otherwise is being paid.

§ 1520.7 Sensitive security information.

Except as otherwise provided in writing by the Under Secretary as necessary in the interest of safety of persons in transportation, the following information and records containing such information constitute sensitive security information:

(a) Any approved, accepted, or standard security program under the rules listed in § 1520.5(a)(1) through (6), and any security program that relates to United States mail to be transported by air (including that of the United States Postal Service and of the Department of Defense); and any comments, instructions, or implementing guidance pertaining thereto.

(b) Security Directives and Information Circulars under § 1542.303 or § 1544.305 of this chapter, and any comments, instructions, or implementing guidance pertaining thereto.

(c) Any selection criteria used in any security screening process, including for persons, baggage, or cargo under the rules listed in § 1520.5(a)(1) through (6).

(d) Any security contingency plan or information and any comments, instructions, or implementing guidance pertaining thereto under the rules listed in § 1520.5(a)(1) through (6).

(e) Technical specifications of any device used for the detection of any deadly or dangerous weapon, explosive, incendiary, or destructive substance under the rules listed in § 1520.5(a)(1) through (6).

(f) A description of, or technical specifications of, objects used to test screening equipment and equipment parameters under the rules listed in § 1520.5(a)(1) through (6).

(g) Technical specifications of any security communications equipment and procedures under the rules listed in § 1520.5(a)(1) through (6).

(h) As to release of information by TSA: Any information that TSA has determined may reveal a systemic vulnerability of the aviation system, or a vulnerability of aviation facilities, to attack. This includes, but is not limited to, details of inspections, investigations, and alleged violations and findings of

violations of 14 CFR parts 107, 108, or 109 and 14 CFR 129.25, 129.26, or 129.27 in effect prior to November 14, 2001 (see 14 CFR parts 60 to 139 revised as of January 1, 2001); or parts 1540, 1542, 1544, 1546, 1548, or § 1550.5 of this chapter, and any information that could lead the disclosure of such details, as follows:

(1) As to events that occurred less than 12 months before the date of the release of the information, the following are not released: the name of an airport where a violation occurred, the regional identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of the aircraft operator in connection with specific locations or specific security procedures. TSA may release summaries of an aircraft operator's total security violations in a specified time range without identifying specific violations. Summaries may include total enforcement actions, total proposed civil penalty amounts, total assessed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA counsel for legal enforcement action, and number of cases closed.

(2) As to events that occurred 12 months or more before the date of the release of information, the specific gate or other location on an airport where an event occurred is not released.

(3) The identity of TSA or FAA special agent who conducted the investigation or inspection.

(4) Security information or data developed during TSA or FAA evaluations of the aircraft operators and

airports and the implementation of the security programs, including aircraft operator and airport inspections and screening point tests or methods for evaluating such tests under the rules listed in § 1520.5(a)(1) through (6).

(i) As to release of information by TSA: Information concerning threats against transportation.

(j) Specific details of aviation security measures whether applied directly by the TSA or entities subject to the rules listed in § 1520.5(a)(1) through (6). This includes, but is not limited to, information concerning specific numbers of Federal Air Marshals, deployments or missions, and the methods involved in such operations.

(k) Any other information, the disclosure of which TSA has prohibited under the criteria of 49 U.S.C. 40119.

(*l*) Any draft, proposed, or recommended change to the information and records identified in this section.

(m) The locations at which particular screening methods or equipment are used under the rules listed in § 1520.5(a)(1) through (6) if TSA determines that the information meets the criteria of 49 U.S.C. 40119.

(n) Any screener test used under the rules listed in § 1520.5(a)(1) through (6).

(o) Scores of tests administered under the rules listed in § 1520.5(a)(1) through (6).

(p) Performance data from screening systems, and from testing of screening systems under the rules listed in § 1520.5(a)(1) through (6).

(q) Threat images and descriptions of threat images for threat image projection systems under the rules listed in § 1520.5(a)(1) through (6).

(r) Information in a vulnerability assessment that has been authorized, approved, or funded by DOT, irrespective of mode of transportation.