No. 13-894

IN THE

Supreme Court of the United States

DEPARTMENT OF HOMELAND SECURITY,

Petitioner,

v.

ROBERT J. MACLEAN,

Respondent.

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

BRIEF FOR *AMICI CURIAE* FORMER U.S. GOVERNMENT OFFICIALS IN SUPPORT OF RESPONDENT

JON L. MILLS
BOIES, SCHILLER & FLEXNER LLP
100 SE Second Street
Suite 2800
Miami, FL 33131

KAREN Y. PAIK
BOIES, SCHILLER & FLEXNER LLP
401 Wilshire Boulevard
Suite 850
Santa Monica, CA 90401

MICHAEL J. GOTTLIEB
Counsel of Record
BOIES, SCHILLER & FLEXNER LLP
5301 Wisconsin Ave., N.W.
Washington, DC 20015
(202) 237-2727
mgottlieb@bsfllp.com

MATTHEW R. SHAHABIAN
BOIES, SCHILLER & FLEXNER LLP
575 Lexington Avenue
New York, NY 10022

Counsel for Amici Curiae

September 29, 2014

QUESTION PRESENTED

The Whistleblower Protection Act ("WPA") shields federal employees from discipline or retaliation if they disclose information that reveals "any violation of any law, rule, or regulation" or a "substantial and specific danger to public health or safety." 5 U.S.C. § 2302(b)(8)(A). The Act exempts from its protection any disclosure of information that has been prohibited by Executive Order in the interest of national defense or foreign affairs, and also any disclosure "specifically prohibited by law." *Id.*

The Department of Homeland Security has issued regulations that prohibit the disclosure of 16 categories of unclassified information that, collectively, are known as "Sensitive Security Information" ("SSI"). *See* 49 C.F.R. pt. 1520. The question is whether an employee who discloses SSI for lawful purposes under the WPA may nonetheless be terminated for making a "disclosure [that is] specifically prohibited by law."

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Administrative Materials

Legislative Materials

Other Authorities

INTEREST OF AMICI CURIAE[1]

Amici are former U.S. Government officials who have served in various capacities in military, diplomatic, intelligence, and other government offices, and who remain committed to advancing our nation's safety and security. The Appendix lists the names of amici and their relevant former and current positions.

Amici respectfully submit this brief in support of the Respondent because their experience leads them to conclude that the Department of Homeland Security's ("DHS") restrictive interpretation of the Whistleblower Protection Act ("WPA") is unnecessary to protect national security or public safety. Indeed, amici fear that DHS's position, if adopted by this Court, would exacerbate excessive secrecy within the Executive Branch, which makes our government less effective.

Amici do not support the public release of classified information, and believe that appropriate limits must be enforced on disclosures made by federal employees. But this case is not about classified information; it is about unclassified information, and the lengths to which executive departments and agencies may go to punish employees who disclose it in alerting Congress, the press, or the public at large about fraud, abuse, or imminent danger. Amici believe

---

[1] No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No persons other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission. Letters from the parties consenting to the filing of *amicus* briefs have been filed with the Clerk of the Court.

that unless Congress explicitly declares otherwise, "sensitive but unclassified" information should not be categorically exempt from whistleblower protection where disclosures have historically helped to expose government wrongdoing and inefficiency, and to prevent great harm to national security.

SUMMARY OF ARGUMENT

The question in this case is whether the WPA allows executive agencies to fire or otherwise discipline their employees for disclosing "Sensitive Security Information" ("SSI"), an amorphous species of unclassified information whose contents are defined solely on the basis of agency discretion. If the position DHS has advanced in this matter prevails, a determination by one bureaucrat that information is "sensitive" will allow the agency to preclude its disclosure indefinitely, and to terminate a whistleblower even where a disclosure saves lives or uncovers criminal behavior. The WPA was not designed to shield so broad a category of information from public disclosure, and this Court should not be persuaded otherwise by the ominous predictions DHS has offered.

The WPA protects the disclosure of information that exposes any "violation of any law, rule, or regulation," "gross mismanagement," or "a substantial and specific danger to public health or safety." *See* 5 U.S.C. § 2302(b)(8).[2] As relevant here, the Act excludes two categories of information from statutory protection: first, any information that is "specifically

---

[2] This provision was first enacted in the Civil Service Reform Act, but it is commonly referred to as part of the WPA, and this brief adopts that terminology.

required by Executive order to be kept secret in the interest of national defense or the conduct of foreign affairs," and second, any disclosure that is "specifically prohibited by law." *Id.* § 2302(b)(8)(A). Although the question presented directly addresses the second exception, it cannot be answered without understanding how both exceptions operate within the context of the national security state.

Congress enacted the WPA, in part, because executive agencies can have little patience for individuals who come forward with embarrassing, dangerous, or unlawful agency practices. The Act's structure serves Congress's aim to eliminate agency discretion to define the types of disclosures that warrant termination or other serious discipline. But Congress has also recognized the need to limit what kinds of information employees may reveal. Thus, the WPA exempts entire agencies that operate in the intelligence community, such as the Central Intelligence Agency and National Security Agency, *id.* § 2302(a)(2)(C), and it excludes specific categories of information such as protected "critical infrastructure information," *see* 6 U.S.C. § 133(a). The WPA has never exempted, however, DHS or its component agency, the Transportation Security Administration ("TSA"), nor has it ever specifically prohibited the disclosure of SSI.

The WPA also relies upon its Executive Order exception to ensure that whistleblower protections do not unduly interfere with national security interests. Presidents have long overseen the federal classification system, which prohibits by Executive Order the public disclosure of information that relates to intelligence, military planning and operations, foreign policy, and other national security interests. DHS

possesses the authority to classify information relating to the safety and security of the transportation system under these orders. *See* Exec. Order No. 13,292, § 1.4(g), 68 Fed. Reg. 15,315 (Mar. 28, 2003); Exec. Order No. 13,284, § 20, 68 Fed. Reg. 4075 (Jan. 28, 2003).

The federal classification system has been criticized for being unnecessarily expansive, but it also contains substantial procedural limitations and safeguards. For example, classified information must be clearly designated by trained individuals known as "classifying authorities," of whom there are only a finite number at any given time, and the classification process includes mandated declassification procedures and meaningful oversight.

Although SSI is not classified under the Executive Order scheme, DHS asks this Court to treat it as such for purposes of the WPA. But DHS's view, if accepted, would grant it more power to exempt information from WPA coverage than the Act vests in the President. While the WPA restricts the President's ability to exempt, via Executive Order, only that information which relates to the national defense or foreign affairs, SSI contains no such limitations. By its own terms, SSI includes confidential commercial and personal privacy information that likely falls outside of the President's national defense or foreign affairs powers.

Although SSI represents a more expansive universe of information than can be classified by Executive Order, it offers few, if any, of the vital procedural protections afforded by the classification process. DHS regulations treat SSI as "secret" upon creation; they do not provide for an automatic "declassification" process; and they offer no limit to what SSI

might cover given the agency's discretion to redefine the category at will.

DHS warns that unless SSI is excluded from the WPA's full protections, federal employees will be "embolden[ed] . . . to disclose SSI," and thereby "put lives at risk." Pet. Br. at 38. Amici's experiences in government have left a markedly different impression. SSI serves valid purposes, and well-intentioned federal employees do their best to protect information that is so defined. Unfortunately, SSI in practice remains ill-defined, susceptible to abuse, and in many ways redundant with other tools that remain available for shielding sensitive information from disclosure. Indeed, much of the information that SSI purports to shield is either classified by Executive Order or specifically precluded from disclosure by existing statutes.

The Executive Branch is not plagued by problems of inflexible authorities, under-classification, or too much information sharing—in each respect, the problem is the opposite. The 9/11 Commission Report famously concluded that excessive secrecy prohibited federal agencies from sharing critical information with each other, and also that "publicity about Moussaoui's arrest and a possible hijacking threat might have derailed the plot." *See* Final Report of the National Commission on Terrorist Attacks upon the United States 276 (2004) (the "9/11 Commission Report"). Along the same lines, the WPA recognizes that national security will not be served by burying reports of imminent public danger or government fraud deep within lengthy internal agency review processes. Had Congress trusted such processes to vindicate the Act's objectives, the WPA would not have protected public disclosures at all.

Exempting SSI from WPA coverage would encourage DHS and other agencies with similar regimes to conceal more and more information within confusing and expansive regulatory categories. Such a result would be inconsistent with the interests of transparency and national security.

ARGUMENT

The WPA protects federal employees who disclose sensitive but unclassified information so long as the disclosure reveals a violation of law, gross inefficiency or danger to public health or safety. The WPA offers such protection here because SSI is not defined or policed by either an Act of Congress or an Executive Order. That interpretation of the WPA, which the Federal Circuit adopted below, is entirely consistent with the design of the federal system that regulates and protects classified information, and it advances the interests of public safety and national security.

SSI was designed to be distinct in every meaningful respect from the Executive Branch's classified information regime, having been created primarily to allow agencies to share certain information without having to comply with requests filed under the Freedom of Information Act ("FOIA"). The structure and history of the classification system as a whole, including SSI's place in it, demonstrate why SSI was not intended, and should not be interpreted, to be exempt from the WPA's protections.

I. THE WPA PROHIBITS FEDERAL AGENCIES FROM DISCIPLINING WHISTLEBLOWERS FOR DISCLOSING INFORMATION THAT THE AGENCY HAS WITHHELD FROM THE PUBLIC BASED ENTIRELY UPON ITS EXERCISE OF DISCRETION

The WPA prevents executive agencies from punishing or intimidating good faith whistleblowers. The structure and history[3] of the Act's narrow exceptions, *see* 5 U.S.C. § 2302(b)(8)(A), reveal Congress's distrust for unbounded agency discretion. Indeed, the context in which the WPA was enacted reinforces that Congress could not have intended to allow agency discretion to define the reach of the Act's protections.

Congress designed the WPA to reduce the problem of excessive secrecy in government by offering federal whistleblowers protections for helping to "uncover and correct administrative abuses." S. Rep. No. 95-969, at 8 (1978) (the "WPA Senate Report"); *see also id.* (seeking to encourage federal employees to "summon[] the courage to disclose the truth"). By the time it enacted the WPA in 1978, Congress was aware of the threat posed by transnational terrorism, and had only recently created legislation to respond to hijackings and bombings of the American airline system. Four years earlier, Congress had enacted the Antihijacking Act and Air Transportation Security Act of 1974, which conferred broad discretion on

---

[3] The parties have briefed extensively the interpretation of the WPA's text, and amici do not repeat those arguments here. *See* Pet. Br. 18-34; Resp. Br. 19-47.

the Federal Aviation Administration ("FAA") to institute increased security measures, including to exempt SSI from FOIA disclosures. Pub. L. No. 93-366, § 202, 88 Stat. 409, 417.

When it considered the WPA, Congress was on notice of the FAA's 1976 published regulations defining what would eventually be called SSI. *See* FAA, Release of Security Information, 41 Fed. Reg. 26,579 (proposed June 28, 1976). Notwithstanding the FAA's SSI definitions,[4] Congress considered and chose to exclude from the final WPA exception the words "rules or regulations," added the term "specifically," and unequivocally stated in its joint committee report that the phrase "specifically prohibited by law" "does not refer to agency rules and regulations." *See* H.R. Rep. No. 95-1717, at 130 (1978) (Conf. Rep.) (the "WPA Conference Report").

Moreover, at the time the WPA was enacted, the phrase "specifically prohibited by law" was generally understood to refer to statutory prohibitions that did not depend on the exercise of absolute agency discretion. Just prior to the WPA's enactment, Congress had enacted the 1976 amendment to FOIA's Exemption 3. The amendment permitted agencies to withhold information "specifically exempted from disclosure by statute," but added the proviso "that such statute [] requires that the matters be withheld from the public in such a manner as to leave no discretion

---

[4] *See also* Report of the Commission on Protecting and Reducing Government Secrecy, S. Doc. No. 105-2, at 5 (1997) (the "Moynihan Commission Report") ("In 1971, a House subcommittee found no fewer than 62 different control markings being used to restrict the distribution of sensitive unclassified information [that were] . . . not linked to any explicit statutory authority.")

on the issue, or [] establishes particular criteria for withholding or refers to particular types of matters to be withheld." *See* Government in the Sunshine Act, Pub. L. No. 94-409, § 3, 90 Stat. 1241, 1242 (1976) (the "FOIA Amendment"). The purpose of the FOIA Amendment was to "overrule the decision of the Supreme Court in *Administrator, FAA v. Robertson*, 422 U.S. 255 (1975)." *See* H.R. Rep. No. 94-1441, at 14 (1976) (Conf. Rep.). *Robertson* held that section 1103 of the Federal Aviation Act of 1958 satisfied FOIA Exemption 3 even though it broadly permitted the agency to "order such information withheld from public disclosure when, in their judgment, a disclosure of such information would adversely affect the interests of such person and is not required in the interest of the public." *See Robertson*, 422 U.S. at 266-67; 49 U.S.C. § 1504.

Prior to the congressional debate and ultimate enactment of the WPA in October of 1978, circuit courts had uniformly concluded that the FOIA Amendment effectively overruled *Robertson*, even for cases that were pending when the Amendment became law. *See, e.g., Am. Jewish Cong. v. Kreps*, 574 F.2d 624, 626-27 (D.C. Cir. Mar. 15, 1978); *Lee Pharms. v. Kreps*, 577 F.2d 610, 614-618 (9th Cir. Jun. 29, 1978). Those courts' decisions adopted the narrow interpretation of "specifically exempted . . . by statute" that a number of courts had applied before *Robertson*. *See, e.g.*, *Stretch v. Weinberger*, 495 F.2d 639 (3d Cir. 1974); H.R. Rep. No. 94-1441, at 14 (1976) (Conf. Rep.) (endorsing *Stretch* result). In the wake of these cases, the Senate's WPA report embraced the FOIA Amendment's narrow interpretation of what constitutes a "specific" statutory exemption, and explained that any qualifying statute under

the WPA must satisfy that standard. *See* WPA Senate Report at 21.

By the time both the House and Senate committees reconciled the meaning of "specifically prohibited by law" in October 1978, therefore, both the courts and Congress understood that the narrow specificity standard applied in all FOIA Exemption 3 cases, including cases filed both before and after *Robertson*. This history best explains Congress's reference "to statutory law *and court interpretations of statute*." *See* WPA Conference Report at 130 (emphasis added). And it shows why DHS's argument—that Congress selected the phrase "specifically prohibited by law" in order to reinstate *Robertson's* holding—is irreconcilable with both judicial and legislative history. *See* Pet. Br. at 28-34.

Congress has since amended the WPA several times. Every time, it has done so to strengthen whistleblower protections, reflecting its desire to encourage public disclosures of agency abuse.[5] In none of these amendments did Congress enact language specifically prohibiting the disclosure of information deemed "sensitive" by the exercise of agency discre-

---

[5] *See* Whistleblower Protection Act of 1989, Pub. L. No. 101-12, § 2(b), 103 Stat. 16, 16 (1989) ("strengthen[ing] and improv[ing] protection for the rights of Federal employees[] to prevent reprisals"); An Act to Reauthorize the Office of Special Counsel, and for Other Purposes, Pub. L. No. 103-424, 108 Stat. 4361 (1994), H.R. Rep. No. 103-769, at 10 (1994) ("provid[ing] federal employees with greatly expanded whistleblower protections"); Whistleblower Protection Enhancement Act of 2012, Pub. L. No. 112-199, 126 Stat. 1465 ("clarify[ing] the [broad scope of] disclosures of information protected from prohibited personnel practices, [and] requir[ing] a statement in non-disclosure policies, forms, and agreements that such policies, forms, and agreements conform with certain disclosure protections").

tion. The structure and history of the statute shows that Congress wanted the decision to remove whistleblower protection to be made not by the agencies whose mismanagement was subject to exposure, but by Congress and the President. This balance was sensible when the WPA was passed in 1978, and it continues to make sense today.

II. THE WPA'S INCORPORATION OF THE EXECUTIVE ORDER CLASSIFICATION SYSTEM APPROPRIATELY BALANCES THE INTERESTS OF NATIONAL SECURITY AND GOVERNMENTAL TRANSPARENCY

The WPA exempts from the Act's protection the disclosure of all information that is "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). That exception expressly incorporates the classified information infrastructure through which the President has long protected sensitive national security information. *See* WPA Senate Report at 22 ("[D]isclosures which are specifically prohibited by Executive Order 11652 (relating to classified material) are exempted from the coverage of this section.").

Created by President Roosevelt during World War II, *see* Exec. Order No. 8381, 5 Fed. Reg. 1147 (Mar. 26, 1940), the classified information system encompasses different tiers of classification depending on the level of secrecy required. The system in place at the time of the disclosure in this case incorporated, as it does today, the familiar categories of "Top Secret," "Secret," and "Confidential." Exec. Or-

der No. 13,292, § 1.2(a).[6] These classification levels are the exclusive means for designating classified national security information within the U.S. Government. *See id.* § 1.2(b) ("Except as otherwise provided by statute, no other terms shall be used to identify United States classified information.").

The classification regime has evolved to include comprehensive procedures for categorizing, reviewing, and declassifying national security information. For example, every Executive Order on classification has limited the ability to classify information to high-level national security officials and their direct designees. *Compare* Exec. Order No. 8381 (1940) (vesting classification authority in the Secretary of War, Secretary of the Navy, and the President), *with* Exec. Order No. 13,292, § 1.3 (vesting original classification authority in "agency heads and officials designated by the President in the Federal Register" and requiring agency heads to oversee any delegations of authority on an as-needed basis). This prescribed chain of delegation helps to ensure direct accountability for classification decisions.

Furthermore, information cannot be "classified" unless an officer with classifying authority determines that its unauthorized disclosure "reasonably could be expected to result in damage to the national security," damage which the officer must be "able to identify or describe." Exec. Order No. 13,292,

---

[6] Executive Order 13,292, issued by President George W. Bush, was the classification order in effect at the time of MacLean's disclosure in 2003. It has since been replaced by President Obama's Executive Order on classification, Executive Order 13,526. In referring to "the Executive Order," this brief relies on the operative Order of President Bush, except where otherwise noted.

§ 1.1(a)(4). The officer must also follow specific procedural requirements. For example, the classification level must be identified "on the face of each classified document," along with the identity of the classifying authority, the agency and office of origin, a "concise reason for classification," and the date of declassification. *Id.* § 1.6(a). No more information than is necessary in any given document may be classified. *Id.* § 1.6(g). The current classification order creates a presumption in favor of using the lowest possible classification level, and an additional rule that if there is "significant doubt about the need to classify information, it shall not be classified." *See* Exec. Order No. 13,526, §§ 1.1(b), 1.2(c), 75 Fed. Reg. 707 (Jan. 5, 2010). The Order also lays out declassification procedures, which over time have expanded to prevent indefinite classification and create additional oversight of classification decisions. *See* Exec. Order. No. 13,292, §§ 3.1-3.7; Exec. Order No. 13,526, §§ 1.5(d), 3.1-3.7.

Congress has long provided legislative enforcement in support of classification decisions. In addition to incorporating the Executive Order regime into the WPA expressly, Congress has, over time, enacted a variety of statutes that set out serious criminal penalties for disclosing classified information.[7]

DHS has ample authority to classify information under the federal regime. The scope of permissible classification includes information relating to transportation security. *See* Exec. Order No. 13,292, § 1.4(g) (covering information relating to "vulnerabilities or capabilities of systems, installations, infra-

---

[7] *See* 18 U.S.C. §§ 793, 794, 798, 1030(a)(1), 1924; 50 U.S.C. §§ 783, 3121.

structures, projects, plans, or protection services relating to the national security"). Both the Secretary of Homeland Security and a senior DHS official have authority to classify information up to the Top Secret level. *See* Exec. Order No. 13,284, § 20, 68 Fed. Reg. 4075, 4077 (Jan. 28, 2003) (authorizing Secretary of Homeland Security to classify information up to Top Secret); DHS, Classified National Security Information, 68 Fed. Reg. 4073, 4074 (Jan. 27, 2003) (designating "senior agency official" at DHS with Top Secret classification authority). The Secretary and senior agency official can delegate that authority to other DHS national security officials so long as the designees do not redelegate their authority. Exec. Order No. 13,292, § 1.3(c); *see also* Office of Inspector Gen., Dep't of Homeland Sec., Reducing Over-classification of DHS' National Security Information 13 (2013) (the "2013 DHS IG Report") (noting that as of 2010, the Secretary had delegated to 25 DHS personnel authority to designate classified material).

Although the executive classification regime contains the protections described *supra*, classification remains much easier than declassification. Institutional and bureaucratic incentives have produced a system in which secrecy too often trumps transparency. This problem has been apparent for decades, yet repeated efforts to reduce over-classification and pseudo-classification have "barely made a dent, and it is not clear that they ever will." David E. Pozen, *The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information*, 127 Harv. L. Rev. 512, 582 (2013).[8] As the

[8] *See also The Over-classification and Pseudo-classification: Part I, II, and III: Hearing Before the Subcomm. on Intelligence,*

Secretary of Homeland Security openly acknowledged before he assumed his present position:

> The reality is that it is much easier to classify something than to de-classify it, and there are huge bureaucratic biases against de-classifying something once it is classified. Put 10 national security officials in a room to discuss de-classifying a certain fact. They will all say, I'm for transparency in principle, but at least 7 will be concerned about second-order effects, someone will say "this is really hard, we need to think about this some more," the meeting is adjourned, and the 10 officials go on to other more pressing matters.

Jeh Charles Johnson, Keynote Address at the Center on National Security at Fordham Law School 9 (Mar. 18, 2013), *available at* http://www.documentcloud.org/documents/623760-johnson-speech-to-fordham-ls.html.

Thus, even within a classification system that benefits from carefully designed limitations and procedural protections, incentives remain aligned towards excessive secrecy.[9] However troubling these

---

Information, and Terrorism Risk Assessment of the H. Comm. on Homeland Sec., 110th Cong. 7 (2007) (statement of J. William Leonard, Director, Nat'l Archives, Information Security Oversight Office) (concluding, based on a review of "every serious review of the classification system since" 1955, that the U.S. government suffers from a serious over-classification problem).

[9] *See, e.g.,* 9/11 Commission Report at 417 ("Current security requirements nurture overclassification and excessive compartmentation of information among agencies."); Reducing

issues are with respect to classified information, they are far worse with respect to information that is unclassified but controlled by executive agencies.

III. EXEMPTING SSI FROM THE WPA'S PROTECTION WOULD BE FUNDAMENTALLY INCOMPATIBLE WITH THE PURPOSES OF THE ACT

SSI presents far more serious problems than those found in the classification regime. As mentioned above, SSI is a category of unclassified information that is principally administered by TSA. For more than three decades of coexistence with the WPA, neither Congress nor the President has ever specifically exempted SSI from the WPA's reach.

In support of its claim that SSI is exempt from the WPA, DHS relies on 49 U.S.C. § 114(r). But that statute was not designed to address WPA. Rather, Congress sought to exempt SSI from routine document requests that were at that time being lodged and litigated under FOIA. The statute that included what is now Section 114(r) provided:

> *Notwithstanding section 552 of title 5, United States Code, relating to freedom of information*, the [FAA] Administrator shall prescribe such regulations as he may deem necessary to prohibit disclosure of any information obtained or devel-

---

Over-Classification Act, Pub. L. No. 111-258, 124 Stat. 2648 (2010) ("An Act [t]o require the Secretary of Homeland Security to develop a strategy to prevent the over-classification of homeland security and other information and to promote the sharing of unclassified homeland security and other information . . . .").

> oped in the conduct of research and development activities under this subsection if, in the opinion of the Administrator, the disclosure of such 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) would be detrimental to the safety of persons traveling in air transportation.

Air Transportation Security Act of 1974 § 316(d)(2), 88 Stat. at 417 (emphasis added). At that time, the scope of what agencies could refuse to disclose under FOIA was unsettled. This provision clarified that whatever ambiguity might define the contours of those FOIA exemptions, the FAA nonetheless retained broad discretion to exempt information from FOIA requests. *See Pub. Citizen, Inc. v. FAA*, 988 F.2d 186, 195 (D.C. Cir. 1993) (finding that § 114(r)'s "notwithstanding" language evidenced Congress's intent to allow the FAA to withhold information in response to FOIA requests).

After September 11th, Congress transferred SSI rulemaking authority from the FAA to the newly-created TSA, which was later moved from the Department of Transportation ("DOT") to DHS. *See* Aviation and Transportation Security Act, Pub. L. No. 107-71, § 101(e), 115 Stat. 597, 603 (2001); Homeland Security Act, Pub. L. No. 107-296, § 1601, 116 Stat. 2135, 2312 (2002).[10] With each amendment, Congress preserved the "notwithstanding" language referring to FOIA only, and never added language stating that TSA could prohibit the disclo-

---

[10] DOT also uses the SSI designation, pursuant to 49 U.S.C. § 40119(b).

sure of information "notwithstanding" the protections of the WPA.

Congress has never created a specific SSI exemption to the WPA with good reason. Namely, SSI is more problematic, and less appropriate for a WPA exemption, than information classified by Executive Order or clearly prohibited by statute for at least six reasons.

First, SSI is broader as a category than information that may be classified by Executive Order. Current TSA regulations define SSI not only in the terms of its authorizing statute, 49 C.F.R. § 1520.5(a), but as encompassing 16 categories of SSI, *id.* § 1520.5(b)(1)-(16), which extend far beyond information relating to the security of transportation networks. And SSI is not even limited to the categories described in the regulations because of category 16, the catch-all provision, which includes "[a]ny information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s), or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119." *Id.* § 1520.5(b)(16).

The overbreadth of SSI is apparent from the range of disclosures that would be illegal under DHS's position. One SSI subsection prohibits the disclosure of solicited *or unsolicited* bid proposals from government contractors, including any "commercial or financial information" requested by the government from such contractors. *Id.* § 1520.5(b)(14). Thus, under DHS's interpretation, an employee could face reprisal for disclosing high-level officials' acceptance of bribes—or even a private company's *unsuccessful attempt* to bribe an official—in the process of awarding government contracts. *See id.* § 1520.5(b)(14)(i). Another subsection covers

research and development funded, *accepted*, *or recommended* by DHS or DOT, meaning that an employee could be fired for revealing the results of an academic study relating to transportation security that has been entirely funded by and completed at a university, so long as DHS or DOT "recommended" the study. *See id.* § 1520.5(b)(15). Similarly, another provision defines SSI as "details of any security inspection or investigation," meaning that after conducting an airport investigation, a TSA employee could face termination for disclosing the diversion of appropriated security funds in order to increase management bonuses, resulting in substandard security practices in an airport. *See id.* § 1520.5(b)(6)(i). By citing these examples, amici do not mean to suggest that SSI covers only information that is ancillary to security. Rather, the point is that Congress could not have intended to allow any agency to exempt such a vast amount of information from the WPA's reach.

DHS's expansive position is difficult to square with the narrow exception the WPA grants to the President to exempt information from disclosure by Executive Order, which is limited to information relating to "national defense or . . . foreign affairs." 5 U.S.C. § 2302(b)(8)(A). If DHS's interpretation of "specifically prohibited by law" is correct, it would mean that Congress granted the Under Secretary for Transportation Security the power to declare a disclosure to be a fireable offense simply by labeling information—including purely commercial or personal privacy information—as sensitive, even where there is no connection to national security or foreign affairs. *See* 49 U.S.C. § 114(r) (vesting authority to promulgate SSI regulations in the Under Secretary).

It seems unlikely, if not implausible, that Congress intended the phrase "specifically prohibited by law" to vest in sub-Cabinet agency heads greater authority to prohibit disclosures than the WPA grants to the Chief Executive.

Second, while information is not "classified" until a trained national security official judges and marks it as such, *see* Exec. Order No. 13,292, §§ 1.3, 1.6, 5.4, SSI is "born" into that designation before, and even entirely in the absence of, any determination by an expert in national (or transportation) security. *See* Mitchel A. Sollenberger, Cong. Research Serv., RL32425, Sensitive Security Information and Transportation Security: Issues and Congressional Options 6 (2004). Regardless of how a document is created, *any* DHS employee or covered person, including certain private individuals, at *any* time, may determine that a document falls into one of the 16 SSI categories. *See* 49 C.F.R. § 1520.7 (defining "covered persons" as including all employees of DHS and DOT, government contractors, private researchers, and all recipients of SSI); *id.* § 1520.9 (requiring covered persons to protect SSI from disclosure and to mark unmarked SSI).[11] Indeed, this duty applies not only to DHS employees; it extends to any "covered person" who comes across what they should recognize as SSI, regardless of whether that person works for an entirely separate federal agency lacking clear policies regarding SSI. *See id.* §§ 1520.7, 1520.9.

---

[11] *See also* Gov't Accountability Office, GAO-05-677, Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information 4 (2005) ("TSA's regulations allow anyone within TSA to designate information SSI.").

Third, unlike SSI, the classification system has established tools for labeling classified information in a manner that helps categorize the information's relative level of sensitivity, and for encouraging the sharing of unclassified information. The classification system creates levels of clearance based on the sensitivity of the information—the Top Secret, Secret, and Confidential designations—while SSI has no such tiers. Nor does SSI share the classification system's presumptions for (i) classifying no more information than is necessary, or at the lowest possible level, or (ii) not classifying at all unless there is demonstrable need. *See* Exec. Order No. 13,292, § 1.6; Exec. Order No. 13,526, §§ 1.1(b), 1.2(c). Generally, SSI requires no written justification prior to designation. *See* Exec. Order No. 13,292, § 1.6(a). And whereas a challenge to classification can go to the Interagency Security Classification Appeals Panel, any challenges regarding SSI markings remain entirely internal to TSA. *Compare* Exec. Order No. 13,292, § 1.8, *with* Dep't of Homeland Sec., Mgmt. Directive 11056.1, § VI.C.1, D, F (Nov. 3, 2006).

Fourth, while the standard classification system requires the declassification of documents over time, DHS at the time of MacLean's disclosure in 2003 had set no such time limits. *See* DOT, Civil Aviation Security Rules, 67 Fed. Reg. 8340 (Feb. 22, 2002); *see also* Gov't Accountability Office, GAO-05-677, Transportation Security Administration: Clear Policies and Oversight Needed for Designation of Sensitive Security Information 4 (2005) (the "2005 GAO Re-

port") ("Once a document is designated SSI, it can remain designated as SSI in perpetuity . . . .").[12]

Fifth, unlike classified information, DHS employees will often lack notice as to what qualifies as SSI, which as a designation attaches automatically to certain categories of information. DHS can alter the definition of SSI at any time by issuing a new regulation, and the "catch-all" SSI category may leave employees confused as to the kinds of information that might later be determined to be sensitive even if not originally marked as such. *See* 49 C.F.R. § 1520.5(b)(16). Indeed, in this case, MacLean received the information in question via unsecured, unencrypted text message, and DHS declared it to be SSI only after MacLean had disclosed it for the purpose of whistleblowing. *See MacLean v. Dep't of Homeland Sec.*, 714 F.3d 1301, 1304 (Fed. Cir. 2013).

Sixth, although its creation was authorized by statute, there has never been any criminal penalty for the unauthorized disclosure of SSI; only civil penalties are available. *See* DOT, Civil Aviation Security Rules, 67 Fed. Reg. at 8352; DOT & DHS, Protection of Sensitive Security Information, 69 Fed. Reg. 28,066, 28,075 (May 18, 2004); *cf.* 49 U.S.C. § 114(v) (granting DHS authority to seek civil penalties for violations of agency regulations or orders). Conversely, the unauthorized disclosure of classified information can trigger criminal prosecution, which

---

[12] Congress has since required DHS to enact policies to release, "upon request," certain SSI that is three years old unless an exemption applies; thus, absent a FOIA or similar request, information marked SSI remains so indefinitely for whistleblower purposes. *See* Department of Homeland Security Appropriations Act, 2007, Pub. L. No. 109-295, § 525(a)(2), 120 Stat. 1355, 1381-82 (2006).

makes it obvious even in the absence of an express exemption that the WPA's protections would not apply. *See supra* note 7.

Congress's treatment of a separate area of homeland security information, referred to by DHS as "protected critical infrastructure information," or "PCII," further underscores why SSI should not be interpreted as exempt from WPA protection. The Homeland Security Act of 2002 created a procedure for operators of critical infrastructure—such as airports, bridges, and the internet—to submit information regarding infrastructure security weaknesses to DHS, while assuring those participants that their information would not be disclosed. *See* 6 U.S.C. § 133(a).

The statute defines "critical infrastructure information" in specific terms.[13] It also provides:

> Notwithstanding *any other provision of law*, critical infrastructure information . . . that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems . . . shall be exempt from disclosure under . . . the Freedom of Information Act . . . [and] shall not . . . be used or disclosed by any officer or employee of the United States for purposes other than the purposes of this subtitle . . . .

---

[13] "Critical infrastructure information" is information that relates to one of three categories that the statute describes, with considerably more detail than is provided in this note, as potential physical or cyber attacks on critical infrastructure; defenses to potential attacks; and operational weaknesses or repairs that could be exploited in a potential attack. 6 U.S.C. § 131(3).

Id. § 133(a) (emphasis added). An employee who discloses PCII in violation of section 133(a) is subject to termination and can be imprisoned for up to a year. *Id.* § 133(f).

Congress added an exception to the PCII system explicitly permitting DHS and its employees to disclose information that would otherwise be covered by Section 133(a) so long as the information is obtained from an independent source. *See id.* § 133(c) (allowing agency "to use such information in any manner permitted by law"). And to avoid any ambiguity, Congress amended that exception in the Whistleblower Protection Enhancement Act of 2012 to state, "[f]or purposes of this section a permissible use of independently obtained information includes the disclosure of such information under [the WPA]." Pub. L. No. 112-199, § 111, 126 Stat. 1465, 1472; *see also* S. Rep. No. 112-155, at 44-45 (2012) ("[W]hen an employee or applicant covered by the WPA obtains information in a manner not covered by the critical infrastructure information program . . . , disclosure by the employee or applicant of that independently obtained information may be a protected disclosure under the WPA . . . without risk of criminal penalties, even if the same information was also voluntarily submitted to DHS under the critical-infrastructure protection program.").

The PCII statute demonstrates that, even with respect to a category of homeland security information to which Congress attached criminal penalties, it also took care to carve out exceptions where the WPA would still protect disclosures. Given the likely overlap between independently-obtained PCII and SSI, the exception set forth in 6 U.S.C. § 133(c) would make very little sense if Congress understood

SSI to be categorically exempt from the WPA's protections. Furthermore, unlike the broad language in Section 114(r) on which TSA relies for its authority to prohibit the disclosure of SSI, the PCII statute is a clear example of Congress "specifically prohibit[ing disclosure] by law." 5 U.S.C. § 2302(b)(8)(A). It specifies the content that cannot be disclosed, leaving no discretion to the agency. *Compare* 6 U.S.C. § 131(3), *with* 49 U.S.C. § 114(r)(1) (leaving scope of information covered to what the "Under Secretary decides"). And the statute expressly states that federal employees cannot disclose the information except as specified, "notwithstanding any other provision of law." *Compare* 6 U.S.C. § 133(a)(1)(D), *with* 49 U.S.C. § 114(r)(1) (notwithstanding FOIA).

Congress has demonstrated—through PCII, incorporation of the classified information system, and otherwise—that it knows how to eliminate specific categories of critical national security information from the WPA's protections when it so desires. It has never created a specific exemption for SSI. DHS should not be permitted to avoid this reality by reference to SSI regulations that operate entirely at the discretion of the agency and offer none of the procedural protections that apply to the marking and handling classified information.

IV. ALLOWING AGENCIES TO EXEMPT CATEGORIES OF INFORMATION FROM WPA PROTECTION WOULD BE INCONSISTENT WITH NATIONAL SECURITY

Whistleblowing that complies with the WPA increases the transparency and accountability neces-

sary for effective national security governance. DHS's proposal to vest agencies with the power to decide what may be exempted from the WPA is not only unnecessary to protect public safety, it would in fact weaken national security by reducing transparency and accountability.

Excessive secrecy is harmful to national security. "[T]he failure to ensure timely access to government information, subject to carefully delineated exceptions, risks leaving the public uninformed of decisions of great consequence." *See* Moynihan Commission Report at 8; *id.* at XXI ("Excessive secrecy has significant consequences for the national interest when, as a result, policymakers are not fully informed, government is not held accountable for its actions, and the public cannot engage in informed debate."). As the 9/11 Commission concluded, overclassification and a failure to share information across agencies contributed to intelligence gaps in the months before the September 11th attacks. *See* 9/11 Commission Report at 103, 267.

Perhaps unsurprisingly given its lack of clarity or procedural safeguards, SSI has contributed to the problem of excessive government secrecy. SSI has been misunderstood, wrongly applied, and misused to conceal agency mismanagement. In 2004, the Congressional Research Service reported multiple events in which the ambiguous definition of SSI worked to preclude common-sense communication and reporting on security threats. *See* Mitchel A. Sollenberger, Cong. Research Serv., RS21727, Sensitive Security Information (SSI) and Transportation Security: Background and Controversies, 3-6 (2004) ("CRS SSI Report"). In 2005, the Government Accountability Office concluded that "TSA does not

have written policies and procedures, beyond its SSI regulations, providing criteria for determining what constitutes SSI." 2005 GAO Report at 3.

Despite a number of reforms that Congress has enacted to improve SSI management,[14] problems have persisted, and Congress has continued to criticize the "pseudo-classification" that agency markings like SSI exacerbate. For instance, in 2007, a member of Congress was denied the ability to quote from an unclassified DHS survey on domestic radicalization at a public hearing on domestic radicalization because the agency had marked the survey as SSI. *See The Over-classification and Pseudo-classification: Part I, II, and III: Hearing Before the Subcomm. on Intelligence, Info., and Terrorism Risk Assessment of the H. Comm. on Homeland Sec.*, 110th Cong. 1-2 (2007) (statement of Rep. Harman). And in 2011, DHS's own SSI Office Director admitted that an investigation of one FOIA withholding had revealed information marked as SSI "that was not by any stretch of the imagination at all SSI, but was either embarrassing or was something that they just didn't want the other side to know . . . [a]nd there was extreme pressure . . . to mark it as SSI." H. Comm. on Oversight & Gov't Reform, *Pseudo-Classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of the Sensitive Security Information (SSI) Designation* 11-12 (2014) (the "2014 Joint Staff Report"); *see also id.*

---

[14] *See* Department of Homeland Security Appropriations Act, 2006, Pub. L. No. 109-90, § 537, 119 Stat. 2064, 2088 (2005); Department of Homeland Security Appropriations Act, 2007, § 525, 120 Stat. at 1381-82; Department of Homeland Security Appropriations Act, 2010, Pub. L. No. 111-83, § 561, 123 Stat. 2142, 2182 (2009).

(finding that "TSA officials were inconsistent in the application of the designation—sometimes choosing to release information the SSI Office determined to be sensitive security information while in other instances refusing to release potentially embarrassing information the SSI Office did not consider to merit the SSI designation.").

Although this case concerns SSI, the holding that DHS proposes would result in numerous expansive WPA exemptions. Notwithstanding efforts to control the spread of "Controlled Unclassified Information" ("CUI"),[15] President Obama admitted in 2010 that federal agencies continue to "employ ad hoc, agency-specific policies, procedures, and markings to safeguard and control [CUI]," and that the "confusing patchwork has resulted in inconsistent marking and safeguarding of documents, led to unclear or unnecessarily restrictive dissemination policies, and created impediments to authorized information sharing." Exec. Order No. 13,556, § 1, 75 Fed. Reg. 68,675 (Nov. 9, 2010).

The National Archives' Information Security Oversight Office ("ISOO") has catalogued 22 separate designations that agencies use to withhold CUI. *CUI Registry,* Nat'l Archives, *available at*

---

[15] *See, e.g.*, Presidential Memorandum on Guidelines and Requirements in Support of the Information Sharing Environment § 2(c), 2005 Pub. Papers 1863 (Dec. 16, 2005); Presidential Memorandum on Designation and Sharing of Controlled Unclassified Information (CUI), 2008 Pub. Papers 654 (May 7, 2008); Presidential Memorandum on Classified Information and Controlled Unclassified Information § 2(b), 74 Fed. Reg. 26,277 (June 1, 2009); Reports and Recommendations of the Presidential Task Force on Controlled Unclassified Information (Aug. 25, 2009).

http://www.archives.gov/cui/registry/category-list.html. In addition to SSI, these categories include information relating to farming practices, Census data, tax collection, patent information, private information collected by immigration authorities, financial regulation, and foreign trade policy. *See Pseudo-Classification of Executive Branch Documents: Problems with the Transportation Security Administration's Use of the Sensitive Security Information Designation: Hearing Before the Subcomm. on Gov't Operations of the H. Comm. on Oversight & Gov't Reform*, 113th Cong. 27 (2014) (statement of John Fitzpatrick, Director of ISOO) (stating that there are 314 unique citations in law, government-wide policy, or federal regulations that authorize a "vast amount" of controlled, unclassified information). The agencies that control this information respond to incentives not dissimilar from the ones that motivate DHS—a desire to avoid controversial and embarrassing disclosures. If this Court interprets the WPA to allow agencies to use their own CUI designations to bar disclosure by whistleblowers, there will remain scarce information of value that federal employees could legally disclose. This imbalance will harm, not help, national security.

If agencies are allowed to decide for themselves what categories of information warrant WPA exemptions, they will have no incentive to allow public disclosures. The types of disclosures protected by the WPA are invariably embarrassing, and agencies as a general matter prefer to avoid public controversy. Permitting agencies to exempt whole swaths of information from the WPA by virtue of applying an entirely subjective "sensitive" label would effectively allow agencies to fire employees for good-faith expo-

sures of illegal, grossly inefficient, or harmful agency activities. As the Senate Committee considering the WPA in 1978 recognized, the inclusion of "rules or regulations" into the exception would "encourage the adoption of internal procedural regulations against disclosure, and thereby enable an agency to discourage an employee from coming forward with allegations of wrongdoing." *See* WPA Senate Report at 21.[16]

The alternative mechanisms embraced by DHS are no substitute for *public* disclosure. The WPA did not simply seek to inform government lawyers and congressional staffers about agency practices—it hoped to facilitate education that would result in a better informed public, which experience teaches is essential to a secure nation. *See Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Acts of September 11, 2001: Hearings Before the S. Select Comm. on Intelligence and the H. Permanent Select Comm. on Intelligence*, 107th Cong. 683 (2002) (statement of Eleanor Hill, Staff Director of the Cong. Joint Inquiry) ("[T]he record suggests that, prior to September 11, the U.S. intelligence and law enforcement communities were fighting a war against terrorism largely without the benefit of what some would call their most potent weapon in that effort: an alert and committed public.").

Section 2302(b)(8)(A) envisions that whistleblowers will play a limited but vital role in alerting the

---

[16] This same view persists. *See* 2014 Joint Staff Report at 22 ("[T]he Administrator has significant latitude in making SSI determinations. This power, combined with the seemingly arbitrary manner in which SSI is labeled, makes it easy for Administrators to play politics with sensitive information.").

public about threats, corruption, and agency mismanagement where internal processes fail. The available alternative mechanisms for public disclosure, such as FOIA, are not well suited to that task. *See* WPA Senate Report at 8; *cf.* Moynihan Commission Report at 53, 62 ("Many who try to use [FOIA]—even to get information in government files about themselves—routinely wait up to several years before they receive a response."); *see also id.* at XXIV ("in 1992 . . . over $108 million dollars was spent simply to process FOIA requests, many of which yielded little or no material that was actually released").

For similar reasons, recourse through the Office of Special Counsel ("OSC") is insufficient to accomplish the objectives of the WPA. Where a whistleblower seeks to disclose information regarding "a substantial and specific danger to public health or safety," submitting to the OSC process would be completely impractical, because such processes have a 15-day evaluation period, whereas a "substantial and specific danger" by its very nature often requires immediate action. *See* 5 U.S.C. § 2302(b)(8); *Chambers v. Dep't of Interior*, 515 F.3d 1362, 1367-1369 (Fed. Cir. 2008) (holding that harm "is sufficiently substantial and specific to warrant protection under the WPA" when it is "likely to occur in the immediate or near future," rather than "a harm likely to manifest only in the distant future."); Pet. Br. at 36 (citing 5 U.S.C. § 1213(b)). Additionally, Congress has in the past found the OSC—itself an executive agency—unable to protect whistleblowers' interests fully. *See, e.g.,* H.R. Rep. No. 103-769, at 14 (1994) (seeking to "free[] whistleblowers from vulnerability to abuses of discretion by the Office of Special Counsel"); S. Rep.

No. 100-413, at 8 (1988) (finding that OSC had focused its interests on "protecting the 'system'" at the expense of "[a]ssuring employees that the OSC's priority is to protect them from reprisal").

Contrary to DHS's representations, Pet. Br. 38-39, applying the WPA to SSI disclosures would not threaten national security or public safety. DHS has clear authority to mark sensitive transportation security information as classified. *See* Exec. Order No. 13,292, § 1.3(c)(3); 2013 DHS IG Report at 13. Indeed, DHS's concerns about transportation system vulnerabilities, and sensitive lists of vital transportation infrastructure assets, Pet. Br. 38, fall within its authority to classify information relating to "vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security." *See* Exec. Order No. 13,526, § 1.4(g).[17] The President also has authority under the WPA to issue a new Executive Order specifically prohibiting the disclosure of the core of what constitutes SSI relating to national security under the WPA; and the President could exempt fed-

[17] To the extent DHS notes concerns with vulnerability reports and assessments of infrastructure assets, it is not SSI but rather the PCII statute, *supra* at 23-25, which provides the relevant framework by which the government most often protects such information from disclosure. *See* 71 Fed. Reg. 52,262, 52,271 (Sept. 1, 2006) (noting that 85% of critical infrastructure information is not held or controlled by the federal government, and thus subject to protection under the PCII framework); DHS, PCII Program Manual 39 (2009), *available at* http://www.dhs.gov/sites/default/files/publications/pcii-program-procedures-manual_508.pdf (noting that transportation vulnerability assessments originated outside of government may be marked as PCII, protected from disclosure, and shared with federal, state, and local governments).

eral marshals' positions entirely from WPA coverage if security concerns warranted such treatment. *See* 5 U.S.C. §§ 2302(a)(2)(B)-(C), (b)(8)(A).

Of course, if Congress actually wanted to exempt from the WPA *all* information that qualifies as SSI, it could do so. Congress has already enacted specific disclosure prohibitions, with accompanying criminal penalties, for a significant amount of information that SSI purports to cover. *See, e.g.*, 6 U.S.C. §§ 131, 133 (critical infrastructure information); 18 U.S.C. § 1905 (prohibiting disclosure of trade secrets and confidential amounts or sources of income, profits, losses, or expenditures); 5 U.S.C. § 552a(b) (prohibiting disclosure, absent written consent, of personal identifying information, including financial, medical or criminal or employment information); *cf.* 42 U.S.C. §§ 2014(y), 2274, 2277 (prohibiting disclosure of "Restricted Data" related to nuclear energy and weapons). Moreover, under the original 1978 WPA, Congress entirely exempted certain agencies from its protections. *See* Civil Service Reform Act of 1978, Pub. L. No. 95-454, § 101(a), 92 Stat. 1111, 1115 (excluding from Section 2302(b)(8)(A) coverage "the Federal Bureau of Investigation, the Central Intelligence Agency, . . . the National Security Agency"). Congress has since updated that list to add other agencies, but not TSA or DHS. *Compare* Duncan Hunter National Defense Authorization Act for Fiscal Year 2009, Pub. L. No. 110-417, § 931, 122 Stat. 4356, 4575 (2008) (adding National Geospatial-Intelligence Agency); Whistleblower Protection Enhancement Act of 2012 § 105, 126 Stat. at 1468 (adding the Office of the Director of National Intelligence and the National Reconnaissance Office), *with* Homeland Security Act of 2002 § 883, 116 Stat. at 2247

("Nothing in this Act shall be construed as exempting [DHS] from requirements . . . to provide whistleblower protections for employees of the Department."). Thus, Congress has demonstrated its capacity to protect a significant amount of information that qualifies as SSI from disclosure, but it has never chosen to exempt SSI as a whole.

Finally, the WPA only prohibits an agency from retaliating against an employee for disclosing information under specific, and narrowly circumscribed, conditions. *See* 5 U.S.C. § 2302(b)(8). Courts have strictly interpreted the requirements of Section 2302(b)(8), finding in favor of whistleblowers in only a handful of litigated cases. *See* Peter Eisler, *Whistle-Blowers' Rights Get Second Look*, USA Today (Mar. 14, 2010) (citing Government Accountability Project study that between 1994 and 2010, the Federal Circuit had ruled for whistleblowers in only three of 203 cases decided on their merits, and that between 2000 and 2010, the Merit Systems Protection Board has ruled for whistleblowers just three times in 56 cases decided on their merits).[18] DHS's contention that the Federal Circuit's reading of the WPA will risk lives utterly ignores the cautious manner in which federal employees have invoked the Act's protections in practice.

Congress struck the appropriate balance in 1978 between governmental transparency and accountability, on the one hand, and the need to keep certain

---

[18] Throughout the 12-year history of the Transportation Security Administration, there is only one published opinion documenting a TSA whistleblower's successful invocation of Section 2302(b)(8). *See Aquino v. Dep't of Homeland Sec.*, 2014 M.S.P.B. 21, P15-P17 (M.S.P.B. 2014).

national security information secret, on the other. This Court should not disturb that balance by according SSI an across-the-board exemption from the WPA's protections. Making the timely disclosure of important yet unclassified information even more difficult will only serve to harm, not help, national security and public safety.

CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted,

JON L. MILLS
BOIES, SCHILLER
& FLEXNER LLP
100 SE Second Street
Suite 2800
Miami, FL 33131

KAREN Y. PAIK
BOIES, SCHILLER
& FLEXNER LLP
401 Wilshire Boulevard
Suite 850
Santa Monica, CA 90401

MICHAEL J. GOTTLIEB
Counsel of Record
BOIES, SCHILLER
& FLEXNER LLP
5301 Wisconsin Ave, N.W.
Washington, DC 20015
(202) 237-2727
mgottlieb@bsfllp.com

MATTHEW R. SHAHABIAN
BOIES, SCHILLER
& FLEXNER LLP
575 Lexington Avenue
New York, NY 10022

Counsel for Amici Curiae

September 29, 2014

APPENDIX

The former U.S. Government officials who join this brief include the following:

Marion E. Bowman – former Deputy Director, National Counterintelligence Executive; former Deputy General Counsel and Senior Counsel for National Security Law and Director, Intelligence Issues and Policy Group (National Security Branch), Federal Bureau of Investigation; former Captain and Chief of Litigation, U.S. Navy; currently Distinguished Fellow, Center for National Security Law, University of Virginia School of Law

Teresa C. Chambers – U.S. Park Police Chief (ret.)

Lou Fisher – former Senior Specialist in Separation of Powers (including Research Director of the House Iran-Contra Committee), Congressional Research Service; former Specialist in Constitutional Law, the Law Library of Congress; currently Scholar in Residence, the Constitution Project

Michael German – former Special Agent, Federal Bureau of Investigation

Lisa Graves – former Deputy Assistant Attorney General, Office of Legal Policy at the U.S. Department of Justice; currently Executive Director, Center for Media and Democracy

Lawrence Korb – former Assistant Secretary of Defense; currently Senior Fellow, Center for American Progress

J. William Leonard – former Director, Information Security Oversight Office at the National Archives and former Deputy Assistant Secretary of Defense for Security and Information Operations; currently Chief Operating Officer, National Endowment for Democracy

Patrice McDermott – former Archives Technician, Jimmy Carter Presidential Papers Project; former Archives Specialist (Lifecycle Coordinator), National Archives and Records Administration; currently Executive Director, OpenTheGovernment.org

Mandi Murray – U.S. Army National Guard, Brigadier General (ret.)

Molly Bishop Shadel – former Attorney-Advisor, Office of Intelligence Policy and Review at the U.S. Department of Justice; currently Professor of Law, General Faculty and Senior Fellow, Center for National Security Law, at the University of Virginia School of Law

A. Bryan Siebert – former Director, Department of Energy Office of Nuclear and National Security Information

Mitchel A. Sollenberger – former Analyst in American National Government, Congressional Research Service; currently Associate Provost for Undergraduate Programs and Integrative Learning and Associate Professor of Political Science at the University of Michigan, Dearborn

Andrew Wright – former Associate Counsel to the President; former Staff Director, Subcommittee on National Security & Foreign Affairs of the Committee on Oversight & Government Reform

in the U.S. House of Representatives; currently
Associate Professor at Savannah Law School