Order Code RL32425

CRS Report for Congress
Received through the CRS Web

Sensitive Security Information and Transportation Security: Issues and Congressional Options

June 9, 2004

Mitchel A. Sollenberger
Analyst in American National Government
Government and Finance Division

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
09 JUN 2004	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Sensitive Security Information and Transportation Security: Issues and Congressional Options	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **David D. Acker Library, and Knowledge Repository Defense Acquisition University Fort Belvoir, VA 22060**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**18**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

Sensitive Security Information and Transportation Security: Issues and Congressional Options

Summary

As a result of the terrorist attacks of September 11, 2001, Congress passed legislation creating the Transportation Security Administration (TSA). The agency was charged with making improvements to the country's transportation security systems and protecting against future terrorist attacks. TSA was also given the authority to establish regulations for protecting certain information from public disclosure. These regulations govern sensitive security information, or SSI.

The SSI regulations prohibit TSA officials and employees having a "need to know" status from disclosing transportation security information that details security programs and equipment; training and security procedures; vulnerability assessments; or other related information. The regulations pertaining to SSI are exempt from Freedom of Information Act disclosure. TSA is required, however, to provide SSI to authorized congressional committees.

The purpose of the SSI regulations is to restrict information relative to future terrorist attacks. TSA's application of the SSI regulations has, however, resulted in some controversies over airport security procedures, employee accountability, passenger screening, and airport secrecy agreements. Some experts believe that too much information has been kept from the public in these circumstances. TSA states, however, that protecting SSI is warranted because of the need to protect transportation systems.

A fundamental issue in this controversy is the tension between securing the nation's transportation systems and keeping the public informed. Democratic governments benefit from an informed citizenry; however, broad openness may provide potential enemies with information that enables attacks on the transportation infrastructure. What level of risk resulting from public access to SSI is acceptable to policymakers and the public? What alternatives are available to the present system, and what are their strengths and weaknesses?

This report provides background information on and analysis of issues concerning the SSI regulations. Additionally, it identifies the transportation security and information issues at the heart of this debate. Finally, the report outlines and assesses policy options for Congress, including endorsing current regulations, giving greater specificity to TSA's protection requirements, setting time limits for protection, creating an advisory commission, requiring periodic congressional briefings, or establishing an oversight board. This report will be updated as events warrant.

Contents

Sensitive Security Information and Transportation Security: Issues and Congressional Options

Introduction

Democratic governments face a difficult tension in weighing their duty to protect information vital to security concerns while keeping the public informed. The 9/11 terrorist attacks on the World Trade Center and the Pentagon gave greater emphasis to this issue in the context of an immediate need for the federal government to protect the nation from future terrorist attacks.

Given that the 9/11 terrorist attacks were accomplished using commercial airliners as weapons, Congress sought to strengthen transportation security by establishing the Transportation Security Administration (TSA).[1] Congress directed the new agency to assess and protect against threats to the nation's air, land, and maritime transportation systems. In the act creating the new agency, Congress incorporated the concept of *sensitive security information* (SSI) and directed the agency to establish regulations to protect such information from public disclosure when disclosure would detract from the security of the nation's transportation system and the safety of travelers and crews. Accordingly, TSA is faced with finding an appropriate balance between its mandate to protect SSI from disclosure and the need to keep the public adequately informed about transportation security.

The application of SSI regulations issued by the TSA, however, has generated controversy. Some critics charge that the agency has withheld too much information from the public. Pilots, fight attendants, and consumer advocates assert that TSA "is muzzling debate of security initiatives by labeling too many of the agency's policies and reports as too sensitive for public dissemination."[2] For some, the issue is simply a conflict between two arguably legitimate needs — the need for security versus the public's need for open access to information so they can make rational travel and transportation decisions for themselves. Jane E. Kirtley, director of the Silha Center for the Study of Media Ethics and Law at the School of Journalism and Mass Communication at the University of Minnesota encapsulated the problem when she

---

[1] S. 1447, 107th Cong., approved as P.L. 107-71 on November 19, 2001. See also "Remarks on Signing the Aviation and Transportation Security Act," *Weekly Compilation of Presidential Documents*, vo1. 37, Nov. 19, 2001, pp. 1687-88.

[2] Sara Kehaulani Goo, "TSA Faulted for Restricting Information," *Washington Post*, Oct. 10, 2003, p. A11.

said that the issue comes down to whether "our openness was what made us so vulnerable."[3]

With a view to informing congressional debate on whether the TSA has achieved an appropriate balance between security needs and the information needs of the traveling public, this report traces the origin of the SSI concept and its incorporation into TSA transportation security regulations; it explains how the treatment of *sensitive security* information differs from the treatment of *national security* information; it discusses the tensions inherent between the need to protect sensitive information and the need to advise the traveling public adequately on transportation security matters; and it presents and analyzes pertinent legislative policy options that may be of interest to Congress.

SSI and the Development of SSI Regulations

Sensitive security information is information that describes air carrier screening procedures, airport or air carrier security programs, maritime transportation security procedures, or other related transportation security matters. The SSI concept appears in federal statutes that prohibit the disclosure of information obtained or developed in carrying out security activities if the TSA Administrator (formerly the Under Secretary of Transportation for Security) determines that such disclosure would "be detrimental to the safety of passengers in transportation."[4] TSA regulations specify the categories of information that may be protected as SSI.[5] When the TSA designates information as SSI, its disclosure is limited by a strict need-to-know basis as determined by TSA; disclosure restrictions remain in force until revoked by TSA.

Statutory Authority

On November 16, 2001, 63 days after the attacks of September 11, Congress passed the Aviation and Transportation Security Act (ATSA), which the President signed into law on November 19.[6] Under ATSA, Congress created the Transportation Security Administration (TSA) — then an agency of the Department of Transportation, but now located within the Department of Homeland Security — and authorized the agency to make improvements in the country's transportation security.[7]

---

[3] Quoted in Bryon Okada, "Public Will Not Be Told Details of D/FW Breach," *Fort Worth Star-Telegram*, Jan. 24, 2003, p. 1.

[4] 49 U.S.C.§ 114(s)(1) and 49 U.S.C. § 40119(b)(1).

[5] 49 C.F.R. § 1520.7.

[6] S. 1447, 107th Cong., P.L. 107-71. See also "Remarks on Signing the Aviation and Transportation Security Act," *Weekly Compilation of Presidential Documents*, vo1. 37, Nov. 19, 2001, pp. 1687-88.

[7] The act assigns TSA responsibility for inspecting persons and property carried by U.S. aircraft operators and foreign air carriers operating in the U.S. These responsibilities cover

(continued...)

ATSA is codified in Title 49 of the United States Code, which includes two statutory provisions authorizing the SSI regulations. The provisions authorized the Under Secretary of Transportation for Security and the Administrator of the Federal Aviation Administration to establish regulations prohibiting the disclosure of certain transportation security information. The pertinent provisions are as follows:

> **§ 114(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 [49 USCS §§ 44901 et seq.] 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.
>
> **§ 40119. Security and research and development activities**[8]
>
> **(a) Disclosure. —** The Under Secretary of Transportation for Security and the Administrator of the Federal Aviation Administration each shall conduct research (including behavioral research) and development activities appropriate to develop, modify, test, and evaluate a system, procedure, facility, or device to protect passengers and property against acts of criminal violence, aircraft piracy, and terrorism and to ensure security.
>
> (**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

---

[7] (...continued)
the requirements of 49 U.S.C. § 44901 *et seq.* and 49 U.S.C. § 44903 *et seq.*, which pertain to civil aviation security.

[8] Section 40119 was originally enacted in 1974 with the Air Transportation Security Act (88 Stat. 417) and modified in 1990 (104 Stat. 1388-370).

(C) be detrimental to the security of transportation

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

(c) Transfers of duties and powers prohibited. — Except as otherwise provided by law, the Under Secretary may not transfer a duty or power under this section to another department, agency, or instrumentality of the United States Government.

Sometime after the Homeland Security Act of 2002 became law, the Transportation Security Administration, with its associated authorities and responsibilities, was transferred from the Department of Transportation to the Department of Homeland Security.

SSI and Transportation Security Regulations

Before the TSA migrated from the Transportation Department to the Homeland Security Department, however, the Under Secretary for Transportation Security (using his authority under ATSA to "issue, rescind, and revise such regulations as are necessary to carry out the functions of [TSA]"[9]) transferred authority for existing Federal Aviation Administration regulations[10] to the Transportation Security Administration[11] on February 22, 2002.[12] TSA incorporated these regulations into its Transportation Security Regulations (TSRs).[13]

The TSRs contain rules on administration, procedure, and security for air, land, and maritime transportation. Subchapter A, titled "Administrative and Procedural Rules," contains Part 1520, which addresses Sensitive Security Information (SSI). The *Federal Register* describes or defines SSI as including "information about security programs, vulnerability assessments, technical specifications of certain screening equipment and objects used to test screening equipment, and other information."[14] This definition is spelled out in more detail in 49 C.F.R. § 1520.7, which is summarized below.

- Section 1520.7(a) protects any security program "that relates to United States mail to be transported by air."

---

[9] P.L. 107-71, 115 Stat. 597 (2001).

[10] 14 C.F.R., Parts 91, 107, 108, 109, 121, 129, 135, 139, and 191.

[11] 49 C.F.R., Parts 1500, 1520, 1540, 1542, 1544, 1546, 1548, and 1550.

[12] The final rule was published as U.S. Department of Transportation, "Civil Aviation Security Rules," *Federal Register*, vol. 67, Feb. 22, 2002, pp. 8340-84.

[13] The United States Coast Guard has promulgated TSA's SSI regulations. In 33 C.F.R. § 101.405, the Coast Guard has established Maritime Security (MARSEC) Directives that set "mandatory measures" to respond to maritime security threats. The MARSEC Directives are considered SSI in accordance with 49 C.F.R. § 1520.

[14] U.S. Department of Transportation, "Civil Aviation Security Rules," p. 8342.

- Section 1520.7(b) through (d) covers security directives and information circulars, selection criteria used in the security screening process, and security contingency plans and/or instructions pertaining to those plans.
- Section 1520.7(e) through (g) relates to any technical specification of any device or equipment used for security communications, screening, or "detecting deadly or dangerous weapons," including an "explosive, incendiary, or destructive substance."
- Section 1520.7(h) covers the release of information that TSA "has determined may reveal a systemic vulnerability of the aviation system, or a vulnerability of aviation facilities, to attack."
- Section 1520.7(i) protects "information [released by TSA] concerning threats against transportation."
- Section 1520.7(j) protects "details of aviation security measures."
- Section 1520.7(k) and (l) relates to any "information" TSA has prohibited from disclosure under the criteria of 49 U.S.C. 40119, or any draft, proposed, or recommended change to the information or records identified in this section.
- Section 1520.7(m) through (p) covers locations, tests, and scores of tests on all screening methods or equipment.
- Section 1520.7(q) protects "images and descriptions of threat images for threat projection systems."
- Section 1520.7(r) relates to all Department of Transportation information on "vulnerability assessment ... irrespective of mode of transportation."

Section 1520.5 specifies that all airport operators, aircraft operators, foreign air carriers, indirect air carriers, applicants, and other persons who receive SSI must protect it from disclosure. Additionally, TSA may disclose SSI to persons with a "need to know" in order to carry out transportation security duties.[15] SSI may be exempted from disclosure under the Freedom of Information Act.[16] The authorizing statute, however, requires TSA to provide SSI information to congressional committees "authorized to have the information."[17]

Notification

TSRs also include rules for notifying the public, airport operators, and others with transportation system responsibilities when transportation security concerns arise. Section 1542.305 permits TSA to order airport operators to "display and maintain in public areas information concerning foreign airports that ... do not

---

[15] 49 C.F.R. § 1520.5(b).

[16] 49 U.S.C. § 40019(b). See *Public Citizen v. FAA*, 988 F. 2d 186, 194-196 (D.C. Cir. 1993). In cases where a person is facing a charge of violating TSA security regulation(s), the alleged violator may be provided copies of the enforcement investigative report which may contain SSI. See 49 C.F.R. § 1520.3(d).

[17] 49 U.S.C. § 114(2).

maintain and administer effective security measures." These displays do not include SSI.

Sections 1542.303 and 1544.305 authorize TSA to issue *Information Circulars* and *Security Directives*, which may include SSI. These circulars and directives are used to notify airport operators of threats to the aviation transportation system. If additional security measures are required, TSA will issue a Security Directive that sets "mandatory measures" that must be carried out.[18] Airport operators and others who receive Information Circulars or Security Directives must restrict their availability "to those persons with an operational need-to-know."[19]

SSI and Classified National Security Information

The distinctions between Sensitive Security Information (SSI) and classified National Security Information (NSI) are important, on the one hand, with regard to their definitions and contexts, and, on the other hand, with regard to how each is handled. Understanding the following distinctions may help clarify some of the issues and controversies that have arisen in the arena of transportation security.

- SSI arises only in the context of transportation security; NSI, in the context of national security and defense, intelligence, and foreign relations.

- The handling of SSI is governed by regulations issued by the Transportation Security Administration; NIS, by Executive Order 12958.

- SSI is "born" protected: SSI regulations prohibit TSA from making available to the public any transportation information "obtained or developed during security activities or research and development activities."[20] Protecting such information requires no action from TSA officials. Classifying NSI, however, requires government officials to determine, pursuant to E.O. 12958, that the document contains national security, intelligence, or foreign relations information qualifying to be withheld from the public.

- SSI regulations do not set forth specific justifications for protecting transportation security information. E.O. 12958, however, sets forth seven criteria that justify classifying national security information and restricting its availability.[21]

---

[18] 49 C.F.R. § 1542.303(a) & 49 C.F.R. § 1544.305(a).

[19] 49 C.F.R. § 1542.303(f)(1) & 49 C.F.R. § 1544.305(f)(1).

[20] 49 C.F.R. § 1520.1(a).

[21] Section 1.5(a) military plans, weapons systems, or operations; 1.5(b) foreign government information; 1.5(c) intelligence activities (including special activities), sources or methods,

(continued...)

- SSI regulations do not distinguish among classes of information. Currently, all transportation security information is considered SSI and its public disclosure is prohibited. Classified national security information, however, is protected at one of three levels — top secret, secret, or confidential — and access to the information depends on the level of classification and the user's level of clearance.[22]

- SSI regulations do not set time limits for declassification and release. The only provision for the release of SSI is for alleged perpetrators of crimes or their representatives to receive SSI "for the sole purpose of providing the information necessary to prepare a response to the allegations."[23] E.O. 12958, as amended, calls for the establishment of a specific date for declassification of protected national security information. If no date is set on the document, then a 10-year limit is established.[24]

The standards set for the classification and declassification of national security information are arguably higher and more specific than the standards for sensitive security information. The lack of specificity of SSI regulations has raised questions about the withholding and eventual disclosure of transportation security information. Accordingly, we now turn to the tensions that can occur when the government withholds sensitive security information, keeping in mind how the handling of national security information differs from that of sensitive transportation security information.

Safeguarding Transportation Infrastructure vs. Public Access to Information

Democratic governments continually face the difficult problem of weighing their duty to protect information vital to security concerns against their responsibility for keeping the public informed. The terrorist attacks of September 11, 2001, gave greater urgency to this debate in the United States, and the implementation of the ATSA mandate has given it focus. The challenge lies in trying to balance these two

---

[21] (...continued)
or cryptology; 1.5(d) foreign relations or foreign activities of the U.S., including confidential sources; 1.5(e) scientific, technological or economic matters relating to national security; 1.5(f) USG programs for safeguarding nuclear materials or facilities; and 1.5(g) vulnerabilities or capabilities of systems, installations, projects or plans relating to U.S. national security. See E.O. 12958, *Federal Register*, vol. 60, Apr. 20, 1995, p. 19825.

[22] See E.O. 12958, *Federal Register*, vol. 60, Apr. 20, 1995, p. 19825.

[23] 49 C.F.R. § 1520.3(d).

[24] For more information on declassification arrangements, see CRS Report 97-771 GOV, *Security Classification Policy and Procedure: E.O. 12958, as Amended*, by Harold C. Relyea.

goals. As former Central Intelligence Agency (CIA) officer Larry C. Johnson stated, "We live in a free and open society. If someone really wants to get information, they can get it. But there's some information we need to withhold."[25] In this environment, TSA has had to weigh its duty to protect sensitive information while still keeping the public informed.

Over the last two years, TSA has applied the SSI provisions of the Transportation Security Regulations to reduce the risk of vital security information from reaching the wrong hands. In one incident, TSA withheld information about an airport event involving an individual who passed through a security checkpoint without being stopped. The agency stated it was "not going to be issuing any kind of report because anything beyond the most general of comments would lead us into areas which concern sensitive security information."[26] In another incident, TSA and the U.S. attorney's office in Miami dropped a criminal case against a former federal baggage screener charged with stealing from passengers' luggage.[27] The U.S. attorney's office withdrew the charges because a federal judge determined that the defense could cross-examine the prosecution's witnesses, which could raise the possibility of disclosing SSI about TSA security and training procedures.[28]

The tension between protecting transportation security information while keeping the public informed is a continual one. Like other federal agencies, TSA is not alone in trying to deal with this issue. The next two sections analyze in greater detail transportation security and public information issues.

Transportation Security Issues

The primary justification for withholding information from the public has been the concern for travelers' safety. It is maintained that the release of SSI could jeopardize the nation's transportation system. The U.S. government has frequently stated that the protection of SSI "is critical to the United States' efforts to protect the general public from terrorists attacks like those committed on September 11, 2001."[29]

The protection of SSI is arguably more important for TSA because of the planning and precision of the 9/11 attacks. As former National Security Adviser Richard V. Allen noted: "If you simply stripped this incredible act of aggression of everything else and just looked at it from the technical point of view, it was a brilliant

---

[25] Alexis Simendinger, "Educating the Enemy?" *National Journal*, vol. 33, Nov. 17, 2001, p. 3583.

[26] Terri Langford, "Report on Incident at D/FW is Sealed; Agency Cites Security in Withholding Details on Breach, Evacuation," *Dallas Morning News*, Jan. 24, 2003, p. 30A.

[27] *USA v. Washington, et al.*, PACER Service Center, 03-CR-20648-ALL, Nov. 13, 2003.

[28] For more information on these and other controversies surrounding the SSI regulations see CRS Report RS21727, *Sensitive Security Information (SSI) and Transportation Security: Background and Controversies*, by Mitchel A. Sollenberger.

[29] *Dr. Kamyar Kalantar et al., v. Lufthansa German Airlines, et al.,* 276 F. Supp. 2d 5, 8, 2003.

maneuver. It was absolutely brilliant. It exploited every weakness we had."[30] TSA officials state that the release of security and training procedures could aid in the planning of a similar attack, and that the divulgence of any information about TSA's security systems could endanger the entire transportation infrastructure.

The public availability of security information also could increase the plausibility of threats to paralyze transportation systems. The disruption could obstruct TSA's efforts to prevent real threats. Additionally, the related increased costs to TSA, private companies, and the public could be great.[31] Airports have already experienced increased costs "through a combination of factors including new capital projects, unfunded security mandates and environmental demands."[32]

Public Information Issues

As the preceding sections suggest, in a post 9/11 environment, it is arguably appropriate and necessary for the federal government to reevaluate the balance between making information public and the need to protect the nation from terrorist threats. SSI regulations are an attempt to prevent transportation security information from reaching the wrong hands and being used to plan another 9/11 attack.

Some say, however, that the public disclosure of information is not a threat to security, but "the key to it."[33] The disclosure of information has long been held as one of the primary ways to combat fraud and abuse in government. As Supreme Court Justice Louis Brandeis once stated, "Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman."[34]

By this logic, it is possible that SSI protection could reduce public pressure for improving security systems. For example, it has been asserted that baggage screening machines used to detect bombs and other security threats are experiencing a number of "false" hits where something other than a bomb or other security risk causes the machine to make a misidentification.[35] TSA spokeswomen Amy von Walter has

---

[30] Simendinger, "Educating the Enemy?" p. 3582.

[31] See CRS Report RS21047, *Unemployment Related to Terrorist Attacks: Proposals to Assist Affected Workers in the Airlines and Related Industries*, by Paul J. Graney, p. 1.

[32] See Airports Staff, "Airports, Airlines Battle Over Solutions," *Aviation Week*, available from author.

[33] John Podesta, "Bush's Secret Government," *The American Prospect*, vol. 14, Sept. 1, 2003, available at [http://www.prospect.org/print-friendly/print/V14/8/podesta-j.html], visited June 9, 2004.

[34] Louis Brandeis, *Other People's Money and How the Bankers Use it* (New York: F.A. Stokes, 1914; reprint, New York: St. Martin's Press, 1995), p. 89 (page citation is to the reprint edition).

[35] The General Accounting Office reports high "false alarm rates" for the baggage machines. See U.S. General Accounting Office, *Challenges Exist in Stabilizing and Enhancing Passenger and Baggage Screening Operations*, GAO Report GAO-04-440T (Washington:

(continued...)

stated that the problem happens "just about everywhere." The difficulty for the public, however, is that the agency has revealed little information about the problem and measures to correct the problem. TSA relies on transportation security concerns in defense of nondisclosure: "We have to be careful what we say about this because we don't want to give a road map to the bad guys."[36]

Others consider the release of transportation security information an incentive for change. Some say the restriction of information deprives travelers of information that they could use to assess travel risks.[37] Further, these policies might lead to public complacency. As former White House Chief of Staff John Podesta notes, "openness does not destroy security; it is often the key to it. The American people cannot remain vigilant if they remain ignorant."[38]

SSI Policy Options

This section identifies some congressional options with a view to balancing the two values of transportation security and public disclosure. These options include accepting the existing SSI regulations, giving greater specificity to the agency's protection requirements, setting time conditions for ending protection, seeking expert advice, requiring periodic congressional briefings, and establishing an oversight board.

Option 1: Maintain the Status Quo

Congress could leave standing the current authorizing statutes and regulations for SSI. Under this option, TSA appears to have full authority to prohibit the disclosure of SSI to the public. This TSA authority is similar to that of the FAA upheld in the1993 case, *Public Citizen v. FAA*, where an aviation consumer group challenged the FAA's authority to promulgate and withhold from the public its rules on certain sensitive security regulations and programs. In the case, the Court of Appeals for the District of Columbia held that the FAA had the authority to withhold such regulations and programs from the public.[39] The court found "that greater

---

[35] (...continued)
Feb. 12, 2004), pp. 19, 33-34.

[36] Bob von Sternberg, "Sometimes, Your Luggage Lies," *Minneapolis Star-Tribune*, March 28, 2004, p. 1A.

[37] The airline passenger group International Airline Passengers Association has advocated "the need for disclosure of threat information to allow passengers to make their own informed decisions about whether and when to fly." Garrett Hodes, "Terrorist Threats: The Friendly Skies Aren't Too Friendly About Notification," *University of Kansas Law Review*, vol. 46, Jan. 1998, p. 372.

[38] Podesta, "Bush's Secret Government."

[39] 988 F.2d 186, 195-96 (D.C. Cir. 1993).

disclosure would jeopardize passenger safety is more than just a finding of fact — it is a prediction of the likely future effect of disclosure."[40]

The present arrangements have so far raised only minor public complaints.[41] For example, in Des Moines, Iowa, local law enforcement officers and airport officials voiced concerns over airport security agreements, which prohibit local police from commenting on any incident involving SSI that has occurred on airport property without authorization by TSA.[42] After some clarification of the agreement by TSA officials and the creation of a training seminar for Des Moines police, the issue was resolved.[43]

Although the continuation of the current SSI regulations appears to provide adequate protection of vital transportation information, some believe that the increased availability of some transportation security information can be an incentive for constructive change. The belief is that, by making more of some transportation information available, the public can make a stronger or better informed case to the industry and government to improve security weaknesses in the transportation system. In addition, many of the controversies over SSI are largely unknown to the public, and thus, do not constitute a pressing concern. Moreover, the public's lack of information limits public participation in policymaking for, and support of, improved transportation systems security.

Option 2: Create Specific Protection Standards

Congress could require greater specificity for SSI regulations. For example, the vague and highly discretionary "need to know" principle provides no set standard for determining who may receive SSI. A possible solution would be to have TSA create categories of persons who could receive certain SSI information, such as TSA officials, security personnel, private companies, and the public. For example, specific information about a breach in security at an airport check point might be available only to TSA officials and security personnel. Private companies and the public would be provided only generalized reports about the incident.

This approach could provide better control over the details of information publicly released, and minimize its value to potential terrorists. In addition, interested parties would know beforehand the kind of information they would be provided, and what to expect from TSA officials if similar incidents occur. This refinement could also ease public apprehension about security incidents while providing more detailed sensitive information for security personnel.

---

[40] Ibid., at 196.

[41] For information about several of the controversies surrounding SSI, see CRS Report RS21727, *Sensitive Security Information (SSI) and Transportation Security: Background and Controversies*, by Mitchel A. Sollenberger.

[42] Tom Alex, "Secrecy in Airport Security Contract Criticized," *Des Moines Register*, Sept. 27, 2003, p.1A.

[43] See CRS Report RS21727, *Sensitive Security Information (SSI) and Transportation Security: Background and Controversies*, by Mitchel A. Sollenberger, pp. 5-6.

There is at least one limit to this option: some types of information may need to be protected at all times. For example, releasing incident reports to the public may have unintended consequences, such as revealing vital security procedures to potential terrorists.

Option 3: Establish Time Limits for Protection

Congress could have TSA place time limits on the protection of SSI. As noted earlier in this report, classified national security information has specific dates for its declassification. If no date is set on the classified document, then a 10-year limit is established.[44] A similar requirement could be made for certain SSI information. For example, reports of security incidents or breaches at airports might lose SSI protection 10 years after their creation, with the possibility that some portion(s) might selectively continue to have SSI protection for an additional number of years. Thus, such a report might be publicly released after 10 years, but with a paragraph or a few sentences redacted. Other reports, such as upgraded security contingency plans, vulnerability assessments, or information pertaining to research and development projects, could be released after a longer period of protection. Nonetheless, allowing for the public disclosure of certain kinds of reports, documents, and records containing SSI after 10 years would make important materials available to, among others, taxpayers, historians, and policy analysts.

Option 4: Create an Advisory Commission

Congress could establish an advisory commission or committee to study SSI security arrangements and provide recommendations. Such a panel was most recently created by Congress in 1994 — the Commission on Protecting and Reducing Government Secrecy — which largely focused on the classified national security information system.[45] The new study commission might also be tasked with considering the integration of SSI protection arrangements with existing information protection systems, as well as exploring other congressional options identified here, such as establishing time limits for discontinuing protection and strengthening SSI management accountability.

A commission on SSI could offer several benefits. First, the commission option allows for a full study of the SSI without needing to act immediately, while also responding to public pressure. When the commission issues its report, Congress could consider its recommendations and implement them on a selective basis, either immediately, or at a later date. Implementation might occur thru legislative action or voluntary TSA compliance.

The difficulty with this option is that many commission recommendations are often not implemented. In addition, a commission's report may not alleviate public

---

[44] For more information on declassification arrangements, see CRS Report 97-771, *Security Classification Policy and Procedure: E.O. 12958, as Amended*, by Harold C. Relyea.

[45] See 108 Stat. 525. See U.S. Commission on Protecting and Reducing Government Secrecy, *Secrecy: Report of the Commission on Protecting and Reducing Government Secrecy* (Washington: GPO, 1997).

pressure to act. Legislative action would be delayed while waiting for a report. A commission could create even greater public pressure to change the SSI regulations.

Option 5: Require Periodic Congressional Briefings

Congress could require TSA to provide periodic congressional briefings or reports on SSI administration. Similar briefings and reports are currently given to the House and Senate Intelligence Committees, which also require the Director of Central Intelligence, the Secretary of Defense, the Secretary of State, and the Director of the Federal Bureau of Investigation to submit annual reports on intelligence activities. The committees also often request department and agency heads to testify about current intelligence issues.[46] The Senate, when approving nominations, has also expressed its sense that intelligence community officials should keep the Senate Intelligence Committee fully and currently informed with respect to intelligence activities, including anticipated activities and those that "may constitute" violations of constitutional rights or other law.[47] Each intelligence committee may also disclose publicly any information that it determines would serve the "public interest."[48]

Congressional briefings or reports could include details on a variety of SSI matters, such as (1) incidents involving breaches of airport security and airport security agreements; (2) the number of requests and denials for information concerning alleged violators of a legal enforcement action; and (3) lists of legal cases or actions involving SSI regulations.[49]

There are several benefits to requiring briefings or reports on SSI-related issues. Both houses of Congress have established similar briefing systems for intelligence matters; moreover, disputes over the disclosure of SSI should not be problematic because Congress already holds closed hearings on sensitive intelligence matters.[50] Requiring periodic briefings or reports could help Congress identify transportation information in the public interest that should be disclosed.

There also are, however, several drawbacks to this option: a number of committees have oversight authority over TSA. A solution to this problem might be

---

[46] House Rule X, clause 11(c)(2), see *Jefferson's Manual, and Rules of the House of Representative*, 108th Cong., H.Doc. 107-284 (Washington: GPO, 2003) and S.Res. 400, section 4(b), see *A Resolution Establishing A Select Committee On Intelligence*, 94th Congress, available at [http://www.congress.gov/cgi-lis/bdquery], visited April 9, 2004.

[47] S.Res. 400, section 11.

[48] House Rule X, clause 11(g)(1) and S. Res. 400, section 8(a).

[49] An alleged violator of a legal enforcement action has the right to request "copies of portions of the enforcement investigative report (EIR), including sensitive security information." See 49 C.F.R. § 1520.3(d). For more information about airport security incidents and airport security agreements, see CRS Report RS21727, *Sensitive Security Information (SSI) and Transportation Security: Background and Controversies*, by Mitchel A. Sollenberger.

[50] A list of the open and closed hearings for the Senate Intelligence Committee is available at [http://intelligence.senate.gov/hr108.htm], visited June 9, 2004.

to provide in the authorizing statute which committees have jurisdiction to investigate SSI-related matters. Another drawback might be the lack of media and public attention to the issue. Congress might be unwilling to require periodic briefings if the issue does not appear to be a serious concern. In addition, Congress would become overburdened if it tried to manage every matter or controversy arising in each agency. Finally, pursuing this option might entangle Congress and the relevant committees in the public dispute over SSI availability.

Option 6: Establish a Select Oversight Entity

Congress might also consider establishing a select oversight entity with powers to review SSI management and its protection by TSA. A board with similar functions was established in 1994 to settle disputes about the declassification of national security information, the Interagency Security Classification Appeals Panel (ISCAP).[51] The panel's membership includes the Secretaries of State and Defense, the Attorney General, the Director of Central Intelligence, the Archivist of the United States, and the President's Assistant for National Security Affairs. ISCAP is charged with: (1) making final determinations on classification challenges; (2) approving, denying, or amending exemptions from automatic declassification sought by agencies; (3) making final determinations on mandatory declassification review requests appealed to it; and, (4) generally, advising and assisting the President regarding these matters. There is also the Information Security Oversight Office (ISOO), mandated by E.O. 12958, which monitors executive branch security classification and declassification policy and practices, and related matters.

Congress could create a similar entity, or designate an existing one, to monitor SSI administration. The entity could have final authority on all SSI-related issues, deciding to either reject or accept protection justifications made by TSA. The board could also make recommendations for improving current SSI management and, generally, advise Congress on ways to protect transportation security while providing the public needed information.

There are several benefits to this option. First, it would establish a system for reviewing all SSI protection decisions. In addition, the entity might alleviate SSI management criticism. This option, however, could create added pressure when entity leadership is considered. Former TSA or other transportation officials might make up a large percentage of a board because of their expertise in the field of transportation security. An unbalanced membership could create even more criticism. A solution could be to established a review board similar to the one created by Congress to re-examine President John F. Kennedy assassination records that were still regarded as too sensitive to open to the public.[52] Although the JFK review board was presidentially appointed, the act required the President to select board members from a list of names submitted by four professional associations: the American Historical Association, the Organization of American Historians, the

---

[51] See EO 12958, 60 Fed. Reg. 19825, *Federal Register,* vol. 60, Apr. 20, 1995, p. 19825.

[52] President John F. Kennedy Assassination Records Collection Act of 1992, P.L. 102-526.

Society of American Archivists, and the American Bar Association.[53] Such a model could be reproduced for a SSI review board.

There is, however, a final drawback potentially inherent in this option: review by an oversight board may be too time-consuming for the release of information in the public interest. By the time review occurs, the usefulness of the information may have passed.

The options identified here offer courses of action which Congress may pursue with a view to balancing the need to protect sensitive transportation security information and the realization of the people's right to know about the policies, activities, and operations of their government regarding transportation security. Each option has demonstrated strengths and weaknesses. TSA and its SSI regulations have been in existence in their present forms for less than three years. The agency has demonstrated its willingness to work with complainants to make adjustments of its SSI regulations and their application, but TSA's cooperation may not be sufficient to realize a successful balance between transportation security needs and the public's need for information. In this event Congress may choose to examine these or other options that could provide a resolution to this issue of SSI information.

[53] P.L. 102-562, sec. 7.