Reconciling Security, Disclosure, and Record-Retention Requirements in Transit Procurements

DETAILS

79 pages | | PAPERBACK

ISBN 978-0-309-15483-3 | DOI 10.17226/14404

AUTHORS

August 2010

TRANSIT COOPERATIVE RESEARCH PROGRAM
Sponsored by the Federal Transit Administration

Responsible Senior Program Officer: Gwen Chisholm Smith

Legal Research Digest 32

RECONCILING SECURITY, DISCLOSURE, AND RECORD-RETENTION REQUIREMENTS IN TRANSIT PROCUREMENTS

This report was prepared under TCRP Project J-5, "Legal Aspects of Transit and Intermodal Transportation Programs," for which the Transportation Research Board is the agency coordinating the research. The report was prepared by Jocelyn K. Waite, Esq., Waite & Associates. James B. McDaniel, TRB Counsel for Legal Research Projects, was the principal investigator and content editor.

The Problem and Its Solution

The nation's 6,000 plus transit agencies need to have access to a program that can provide authoritatively researched, specific, limited-scope studies of legal issues and problems having national significance and application to their business. Some transit programs involve legal problems and issues that are not shared with other modes; as, for example, compliance with transit-equipment and operations guidelines, FTA financing initiatives, private-sector programs, and labor or environmental standards relating to transit operations. Also, much of the information that is needed by transit attorneys to address legal concerns is scattered and fragmented. Consequently, it would be helpful to the transit lawyer to have well-resourced and well-documented reports on specific legal topics available to the transit legal community.

The *Legal Research Digests* (LRDs) are developed to assist transit attorneys in dealing with the myriad of initiatives and problems associated with transit start-up and operations, as well as with day-to-day legal work. The LRDs address such issues as eminent domain, civil rights, constitutional rights, contracting, environmental concerns, labor, procurement, risk management, security, tort liability, and zoning. The transit legal research, when conducted through the TRB's legal studies process, either collects primary data that generally are not available elsewhere or performs analysis of existing literature.

Applications

Transit agencies have historically been aware of the confidentiality required in the bidding process. More recently, maintaining the confidentiality of security information not commonly available has come to the fore. While issues related to such security information are most obvious for security contracts, transit agency personnel should also be aware of the potential for security information being included in competitive bidding for other types of contracts. At the same time, there is also a clear, well-established public interest in ensuring that publicly funded projects are transparent.

There are several major aspects of the procurement process for which it is important to be cognizant of security requirements: developing the procurement documentation, allowing site visits and access to ancillary documents not part of the procurement documentation, responding to requests for information from parties other than bidders and contractors, and managing procurement documents.

Transit agencies must also be cognizant of disclosure requirements under both federal and state law that will affect their ability to protect security information.

There are requirements relevant to transit agencies' efforts to balance the competing needs of open government and public security. These legal requirements include federal and state open records requirements, including security exemptions; post-September 11, 2001, federal requirements for specified types of security information; and federal and state record retention requirements.

This digest should be useful to attorneys, transportation officials, engineers, information specialists, security personnel, record retention staff, and policy makers.

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

CONTENTS

LIST OF ACRONYMS

All departmental references are to federal agencies unless otherwise specified in the report.

ATSA	Aviation and Transportation Security Act of 2001
C.F.R.	Code of Federal Regulations
CII	Critical Infrastructure Information
CIIA	Critical Infrastructure Information Act of 2002
DOJ	Department of Justice
DHS	Department of Homeland Security
DOT	Department of Transportation
FBI	Federal Bureau of Investigation
FTA	Federal Transit Administration
FOIA	Freedom of Information Act
GAO	Government Accountability Office
HIPAA	Health Insurance Portability and Accountability Act
HSA	Homeland Security Act of 2002
IFR	Interim Final Rule
MD	Management Directive
NTSSA	National Transit Systems Security Act of 2007
NDA	Nondisclosure Agreement
NPRM	Notice of Proposed Rulemaking
SSMP	Safety and Security Management Plan (plan provided for under FTA guidance implementing project management plan required under section 5327(a))
SSI	Sensitive Security Information
TSA	Transportation Security Administration
U.S.C.	United States Code

LIKELY QUESTIONS CONCERNING MANAGEMENT OF SECURITY INFORMATION

Many transit agencies are not familiar with federal requirements for managing security-related information, particularly the technical requirements for critical infrastructure information (CII) and sensitive security information (SSI). Several likely questions, along with sections of the report where the topics are discussed, are set forth below.

1. What are the statutory requirements that cause information to be considered protected CII or SSI under federal law? Are the two categories of information equally relevant for transit agencies? *See* Section II.B, Critical Infrastructure Information/Sensitive Security Information.

2. What are the major SSI-related issues of which transit agencies should be aware? *See* the introductory portion of Section II.B, Critical Infrastructure Information/Sensitive Security Information.

3. Are transit agencies required to maintain the confidentiality of infrastructure information the agencies themselves submit to the federal government? *See* the introductory portion of Section II.B, Critical Infrastructure Information/Sensitive Security Information; discussion of the Critical Infrastructure Information Act of 2002 in Section II.B.1, Federal Legislation.

4. What is the relationship between Federal CII and SSI requirements and state disclosure requirements? *See* Section III.B, Public Records Laws—Security Exemptions and Section III.C, Public Records Laws—Other Exemptions That May Protect SSI and Other Security Information.

5. What steps should transit agencies take to protect SSI and Restricted Security Information (information that does not meet the federal definition of SSI but is nonetheless worthy of protection from disclosure because of the transportation security ramifications of disclosing it) in the procurement process? *See* Section IV, Transit Agency Practices and Section V, Applying Security and Contract Management Requirements to the Competitive Procurement Process.

RECONCILING SECURITY, DISCLOSURE, AND RECORD-RETENTION REQUIREMENTS IN TRANSIT PROCUREMENTS

By Jocelyn K. Waite, Esq.
Waite & Associates, Reno, Nevada

I. INTRODUCTION

A. Statement of the Problem

Public transportation has been the target of planned and actual terrorist attacks. Part of public transit agencies' security efforts must include taking steps to ensure that information that would facilitate such attacks does not become readily available. At the same time, there is also a clear, well-established public interest in ensuring that publicly-funded projects are transparent and that information to provide oversight is publicly available. This tension plays out in the area of procurement and contract management. Material in bid solicitations, responses, and contracts that contains potentially harmful information not otherwise available must be kept secure, while safeguarding the public interest in open government. Accordingly, public transit agencies must balance the competing legal and public policy interests manifested by requirements for full disclosure of the public's business on the one hand and security concerns on the other.

1. Purpose

In managing competitive security procurements—and in some circumstances nonsecurity procurements with security-related elements—agency personnel responsible for developing and managing procurements must be cognizant of disclosure requirements under federal and state public records laws, as well as the obligation to keep certain information with security implications confidential. These competing needs may influence the structure of procurements. Confidentiality requirements come into play not only in the context of responding to requests for information, but in maintaining adequate records management systems.

The purpose of this digest is to provide government and private attorneys who specialize in procurement and contract management, as well as other attorneys and management personnel, an overview of the legal requirements that are relevant to the process of balancing the competing needs of open government and public security. In particular the digest is intended to provide these practitioners information about federal and state requirements concerning record retention and disclosure, as well as practices transit agencies have adopted to meet their responsibilities in balancing these competing public policy interests. Particularly in terms of state requirements, the digest is intended to provide enough information to allow transit agencies to more easily research the requirements in their specific jurisdictions. The digest is also intended to provide transit agencies a basis for assessing issues they may wish to consider as they develop policies for managing security information throughout the procurement process. Information in the digest is current as of October 2009.

2. Focus

The balance of the Introduction presents the historical background of threats to public transportation and of public records requirements, including in both cases the context of actual attacks, such as the events of September 11, 2001 (9/11). The potential relationship between competitive procurement documents and disclosure requirements is also raised. The main body of the digest examines federal and state records management requirements to the extent that—in the context of competitive bidding—legislation and regulations require transit agencies to keep information from public disclosure, allow transit agencies to keep information from public disclosure, and require transit agencies to disclose information. The digest includes citations to all state freedom of information laws (Appendix B), security exemptions (Appendix C), and state records management laws (Appendix D). As is the case throughout the digest, links to citations are provided for convenience; transit agencies should verify statutory language from official sources.

The digest also discusses several examples of how public transit agencies in fact manage security information in the procurement process in light of the agencies' obligations regarding disclosure of public records. Due to the sensitivity of this information, not all agencies have been identified. After reviewing federal and state legal requirements, the report presents issues to consider in reviewing agency practices concerning the management of security information during the competitive procurement process.

3. Scope

The digest does not focus on requirements concerning information sharing between government agencies, except to the extent that such requirements are relevant to the public disclosure issue. However, the discussion of federal and state security exemptions should be useful for transit agencies interesting in understanding the scope of their ability to share security information without incurring an obligation to disclose that infor-

mation to the general public. A detailed discussion of required security measures is beyond the scope of the digest.[1]

The digest does not provide a state-by-state analysis on all relevant points; rather, it highlights the issues that transit agencies should consider in devising their policies for handling security information in the procurement and records management processes. Examples of state requirements are provided so that transit agencies can "learn from the experiences and practices of others to find a balance between security requirements and the need for open government."[2]

B. Background of Threats to Public Transit Systems

The background of threats to public transit systems, both in the United States and abroad, provides some context for the need to protect transit security information. This section discusses the general vulnerability of public transit systems to attack, including examples of recent threats, and government response to threats of attack.

A note on terminology: as discussed below, federal legislation defines a class of information as sensitive security information (SSI). (See List of Acronyms.) This is a term of art and is only used in the report to describe information that meets the federal definition. However, it is possible for information not to meet the federal definition of SSI and still be worthy of protection from disclosure because of the transportation security ramifications of disclosing it.[3] Transit agencies routinely protect such information, but the author is not aware of a standard term. Therefore, throughout the report such sensitive but non-SSI information is referred to as "restricted security information." The term "security information" refers to information the disclosure of which is likely to threaten transportation security, and may be used where the distinction between SSI and restricted security information is not legally significant.

1. Vulnerability of Public Transit Systems to Attack/Recent Threats to Public Transit Systems

The openness of transit systems, as opposed to air transport, makes them particularly vulnerable to attack and difficult to secure. For example, transit vehicles that operate above ground, often equipped with large windows and doors, are vulnerable to close-range attack. In addition, transit systems must maintain accessibility, which eliminates some options for hardening access.[4] Rail transit systems in particular present high consequence targets because of the potential loss of life and economic disruption. The Transportation Security Administration (TSA) has identified factors that make rail transit a high-consequence target: large numbers of passengers, confined environment, stations located near or below major government buildings, significant office complexes, and iconic structures.[5]

Worldwide, 182 public transit systems have been subjects of terrorist attacks.[6] Among the most notable of these were a subway bombing in Moscow (February 2004) that killed at least 39 people and injured more than 30 others;[7] bombing of trains in Madrid by Basque separatists in March 2004; a suicide bombing outside a Moscow subway reportedly carried out by an Al Qaeda–affiliated group;[8] and attacks on the London transit system on July 7, 2005, killing about 50 people and injuring more than 700.[9] The London attacks came about

---

[1] Numerous reports discuss recommended security measures, *e.g.*, YUKO NAKANISHI, TRANSIT SECURITY UPDATE, A SYNTHESIS OF TRANSIT PRACTICE (Transportation Research Board, Transit Cooperative Research Program Synthesis 80, 2009), http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_syn_80.pdf; JOHN N. BALOG, ANNABELLE BOYD, & JAMES E. CATON, THE PUBLIC TRANSPORTATION SYSTEM SECURITY AND EMERGENCY PREPAREDNESS PLANNING GUIDE 2003, http://transit-safety.volpe.dot.gov/publications/security/PlanningGuide.pdf. *See also* TRANSTECH MANAGEMENT, INC., GUIDANCE FOR TRANSPORTATION AGENCIES ON MANAGING SENSITIVE INFORMATION (National Cooperative Highway Research Program Report 525: Surface Transportation Security, Vol. 5, Transportation Research Board, 2005), http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_525v5.pdf.

[2] *Right to Know vs. Need to Know: States Are Re-examining Their Public-Records Laws in the Wake of Sept. 11*, Homeland Security Brief, The Council of State Governments, 2003, www.csg.org/pubs/Documents/Brief1003RightToKnow.pdf (accessed Sept. 20, 2009).

[3] *See* TRANSTECH MANAGEMENT, INC., *supra* note 1, at 2. *See* II.B, *infra*, Protected Critical Infrastructure Information (PCII)/Sensitive Security Information (SSI).

[4] MATTHEW RABKIN, ROBERT BRODESKY, FRANK FORD, MARSHA HAINES, JORDAN KARP, KRISTIN LOVEJOY, TERRY REGAN, LINDA SHARPE, & MARGARET ZIRKER, TRANSIT SECURITY DESIGN CONSIDERATIONS, ch. 3, *Security in the Transit Environment* (2004), http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/DesignConsiderations/CD/ftasesc.pdf (accessed Sept. 19, 2009).

[5] Department of Homeland Security, Transportation Security Administration, Proposed Rule, *Rail Transportation Security*, Fed. Reg. 71, No. 245, 76852, 76854, Dec. 21, 2006, http://edocket.access.gpo.gov/2006/pdf/E6-21512.pdf.

[6] Section 1403, Findings, Pub. L. No. 110-53, 121 Stat. 401 (Tit. XIV, Public Transportation Security), codified at 6 U.S.C. § 1132.

[7] *Moscow Mourns Metro Bomb Victims*, CNN, Feb. 7, 2004, www.cnn.com/2004/WORLD/europe/02/07/moscow.blast/index.html (accessed July 30, 2009).

[8] Steven Lee Meyers, *Suicide Bomber Kills 9 at Moscow Subway Station*, N.Y. TIMES, Sept. 1, 2004, www.nytimes.com/2004/09/01/international/europe/01moscow.html (accessed July 30, 2009).

[9] Precise numbers varied, but the death tolls appeared to have been about 50, with many more injured. *Cf.*, Don Van Natta Jr. & David Johnston, *London Bombs Seen as Crude; Death Toll Rises to 49*, N.Y. TIMES, July 9, 2005, www.nytimes.com/2005/07/09/international/europe/09intel.html?scp=5&sq=london%20+%20bomb%20+%202005&st=cse (accessed July 30, 2009); Glenn Frankel & Fred Barbash, *Death Toll From London Blasts Rises: 50 Killed in Attacks, 22 More in Critical Condition*, WASH. POST, July 8, 2005; Statement to

a decade after a Japanese cult had dispersed sarin gas on the Tokyo subway, killing more than 10 people and injuring thousands.[10]

In addition to actual attacks on public transportation elsewhere in the world, there have been various reports of possible attacks on transit systems in the United States. These include possible terrorist plots against the New York City subway system in the fall of 2007[11] and in late 2008.[12]

2. Government Responses to Terror Threats

As might be expected, one government response to terror threats—whether based on a specific threat to an individual system or in response to threats or actual attacks elsewhere—is to increase security. For example, in the wake of the Madrid bombings, TSA issued two security directives in May 2004 to rail transit operators.[13] A portion of these directives became the basis for the Rail Transportation Security Rule issued in 2008.[14] U.S. systems nationwide increased security after the London bombings in 2005.[15]

Transit agencies can increase security by augmenting security personnel, installing video surveillance equipment, and conducting random searches.[16] In addition, they can conduct vulnerability assessments. The Federal Transit Administration (FTA), which does not have the authority to regulate transit agency security operations, has initiated various nonregulatory activities,[17] including measures aimed at increasing security activities.

In addition, FTA's recommendations[18] include a number of actions that relate to protecting security information—either directly or because they require creating security information that must then be protected. These include: Action Item 9, establishing a risk management process to assess and manage threats, vulnerabilities, and consequences; Action Item 14, conducting background checks of employees and contractors;[19] Action Item 15, controlling access to documents of security critical systems; and Action Item 16, developing a process for handling and access to SSI.

As discussed in the following section, both the federal and state governments also reacted to terror threats by enacting limitations on disclosure of otherwise public information, based on security concerns.

C. Background of Public Records Requirements

Historically, public records requirements have been viewed as facilitating public oversight of government activity. The rationale for "sunshine" laws is that democracy requires oversight of government activity, which in turn requires that the general public have access to information about government activity.[20] Justice Black drew the connection between democracy and informed public opinion in a case predating enactment of the Federal Freedom of Information Act (FOIA).[21] When he signed the FOIA in 1966, President Johnson

Parliament on the London Bombings, July 11, 2005, www.number10.gov.uk/Page7903 (accessed July 30, 2009).

[10] JOCELYN WAITE, THE CASE FOR SEARCHES ON PUBLIC TRANSPORTATION 4, n.10 (Transit Cooperative Research Program Legal Research Digest No. 22, 2005), citing U.S. GENERAL ACCOUNTING OFFICE, MASS TRANSIT: CHALLENGES IN SECURING TRANSIT SYSTEMS 7 (2002) (killed 11, injured over 5,000); BRIAN MICHAEL JENKINS & LARRY N. GERSTEN, PROTECTING PUBLIC SURFACE TRANSPORTATION AGAINST TERRORISM AND SERIOUS CRIME: CONTINUING RESEARCH ON BEST SECURITY PRACTICES 49 (MTI Report 01-07, 2001) (killed 12, injured thousands). Jenkins and Gersten provide an in-depth look at the Tokyo attack, at 49–65, http://onlinepubs.trb.org/onlinepubs/tcrp/tcrp_lrd_22.pdf.

[11] *Official: Threat Cited This Weekend*, CNN, Oct. 7, 2005, www.cnn.com/2005/US/10/07/newyork.subways/ (accessed July 30, 2009).

[12] James Gordon Meek, Alison Gendar, & Larry McShane, *FBI Warns of Possible Terror Plot Against New York City Subway System During Holiday Season*, N.Y. DAILY NEWS, Nov. 26, 2008, www.nydailynews.com/news/2008/11/26/2008-11-26_fbi_warns_of_possible_terror_plot_agains.html (accessed July 30, 2009).

[13] Mass Transit and Passenger Rail Security, www.tsa.gov/what_we_do/tsnm/mass_transit/index.shtm.

[14] Rail Transportation Security, Final Rule, 73 Fed. Reg. 72130, Nov. 26, 2008, http://edocket.access.gpo.gov/2008/pdf/E8-27287.pdf (49 C.F.R. pts. 1520 and 1580).

[15] Laura Parker, Charisse Jones, & Thomas Frank, *U.S. Mass-Transit Systems Step Up Vigilance*, USA TODAY, July 7, 2005, www.usatoday.com/news/washington/2005-07-07-dc-londonblasts_x.htm (accessed July 30, 2009).

[16] David Randall Peterman, Bart Elias, & John Frittelli, *Transportation Security: Issues for the 110th Congress*, CRS Report to Congress, RL 33512, Jan. 3, 2007, http://ncseonline.org/NLE/CRSreports/06Dec/RL33512.pdf (accessed July 30, 2009).

[17] Transit security initiatives are described at http://transit-safety.volpe.dot.gov/Security/SecurityInitiatives/default.asp. BALOG, BOYD, & CATON, *supra* note 1.

[18] TSA/FTA Security and Emergency Management Action Items for Transit Agencies, http://transit-safety.volpe.dot.gov/Security/SecurityInitiatives/ActionItems/default.asp; www.tsa.gov/assets/pdf/mass_transit_action_items.pdf.

[19] See additional guidance, http://transit-/safety.volpe.dot.gov/publications/security/AdditionalGuidance/PDF/AdditionalGuidance.pdf.

[20] *See* NLRB v. Robbins Tire & Rubber Co., 437 U.S. 214, 242, 98 S. Ct. 2311, 2327, 57 L. Ed. 2d 159, 178 (1978) ("The basic purpose of [the] FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed.") *See also* Robert Tanner, *States Steadily Close Public Access to Information*, THE WORLD, Mar. 17, 2008, www.theworldlink.com/articles/2008/03/17/news/doc47dead5e03573785159931.txt (accessed Feb. 28, 2009).

[21] "The effective functioning of a free government like ours depends largely on the force of an informed public opinion." Barr v. Matteo, 360 U.S. 564, 577, 79 S. Ct. 1335, 1342, 3 L. Ed. 2d 1434, 1444 (1959) (Justice Black, concurring). Throughout this report the term "FOIA" refers to the federal statute unless otherwise specified.

called out that principle: "Democracy works best when the people have all the information that the security of the Nation permits."[22]

The same principle is at work at the state level.[23] The principle is recognized in state statutes and by state courts.[24] The Alaska Supreme Court declared:

> The cornerstone of a democracy is the ability of its people to question, investigate and monitor the government. Free access to public records is a central building block of our constitutional framework enabling citizen participation in monitoring the machinations of the republic. Conversely, the hallmark of totalitarianism is secrecy and the foundation of tyranny is ignorance.[25]

Yet as important as the public's right to know is, it must be balanced against other interests, such as personal privacy, the need for commercial confidentiality, and—increasingly—security. Balancing security and disclosure considerations requires answering a fundamental question:[26] when does the public's right to know outweigh the potential danger of releasing the information in question? Or vice versa, as the phrasing of the question may indicate the presumption of the questioner: disclosure or nondisclosure.

1. Disclosing Public Records

The presumption under FOIA[27] and most state public records acts, embodying the principles described above, is one of disclosure. The obligation to disclose information under public records law exists so long as the public agencies retain covered public records. Thus the obligation is affected by federal and state laws requiring that public agencies retain public records for specified periods of time. For example, the U.S. Department of Transportation (USDOT) imposes retention and access requirements for records related to awards to recipients.[28] State record retention requirements may be included as part of a comprehensive public records statute[29] or may exist as part of other statutory schemes.

In addition to being protected by state statute, in some states the right to inspect public records is protected by the state constitution. The California state constitution, for example, creates a constitutional right of access to public agency records and calls for strict construction of statutes limiting such access.[30] Other states with constitutional protection of right of access include Florida,[31] Montana,[32] and North Dakota.[33]

1. Effect of 9/11 Attacks

Following the 9/11 attacls, a trend developed at both the federal and state levels toward keeping more government information secret.[34] Both the executive and legislative branches of the federal government supported increased levels of secrecy.

In particular, the Bush administration moved away from the prior FOIA presumption of disclosure under the Clinton administration[35] and under Supreme Court

---

[22] Kristen Elizabeth Uhl, *The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security*, Comment, 53 AM. U. L. REV. 261, 263, n.1 (2003), www.wcl.american.edu/journal/lawrev/53/uhl.pdf?rd=1 (accessed Mar. 4, 2009).

[23] *E.g.*, N.H. REV. STAT. ANN. 91-A:1 Preamble.—Openness in the conduct of public business is essential to a democratic society. The purpose of this chapter is to ensure both the greatest possible public access to the actions, discussions, and records of all public bodies, and their accountability to the people, www.gencourt.state.nh.us/rsa/html/VI/91-A/91-A-1.htm.

[24] *E.g.*, Head v. Colloton, 331 N.W.2d 870, 873–74 (Iowa 1983) (purpose of Iowa open records law: "to open the doors of government to public scrutiny—to prevent government from secreting its decision-making activities from the public, on whose behalf it is its duty to act.").

[25] Fuller v. City of Homer, 75 P.3d 1059, 1062 (Alaska 2003).

[26] Mitchel A. Sollenberger, *Sensitive Security Information and Transportation Security: Issues and Congressional Options*, CRS Reports to Congress, RL32425, June 9, 2004, www.fas.org/sgp/crs/RL32425.pdf.

[27] 5 U.S.C. § 552.

[28] Section 18.42, 49 C.F.R. pt. 18—Uniform administrative requirements for grants and cooperative agreements to State and local governments, http://edocket.access.gpo.gov/cfr_2008/octqtr/pdf/49cfr18.42.pdf. *See* II.C, *Procurement and Contract Management Issues*, *infra* this digest.

[29] *E.g.*, Florida Public Records Statute, §§ 119.01 *et seq*., www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&URL=Ch0119/titl0119.htm&StatuteYear=2008&Title=%2D%3E2008%2D%3EChapter%20119. See III.D., *Record Management Laws*, *infra* this digest.

[30] Michaelis, Montanari & Johnson v. Superior Court, 44 Cal. Rptr. 3d 663, 667, 38 Cal. 4th 1065, 136 P.3d 194 (Cal. 2006), *citing* CAL. CONST. art. I, § 3, subd. (b).

[31] FLA. CONST. art. I, § 24, www.myflsunshine.com/sun.nsf/sunmanual/AB22C5DD97920270852566F30071D093.

[32] MONT. CONST. art. II, § 9 (preserving a right to examine documents "except in cases in which the demand of individual privacy clearly exceeds the merits of public disclosure."), http://leg.mt.gov/css/Laws%20and%20Constitution/Current%20Constitution.asp.

[33] N.D. CONST., art. XI, § 6 (protects the right to protect public records unless otherwise provided by law), www.legis.nd.gov/constitution/const.pdf.

[34] GINA MARIE STEVENS & TODD B. TATELMAN, PROTECTION OF SECURITY-RELATED INFORMATION, CRS Report for Congress RL33670, CRS-1 (2006), www.fas.org/sgp/crs/secrecy/RL33670.pdf (accessed Mar. 4, 2009).

[35] Uhl, *supra* note 22, at 272–74; 285–87; GENEVIEVE J. KNEZO, "SENSITIVE BUT UNCLASSIFIED" AND OTHER FEDERAL SECURITY CONTROLS ON SCIENTIFIC AND TECHNICAL INFORMATION: HISTORY AND CURRENT CONTROVERSY, CRS Report for Congress, RL31845, CRS-23–CRS-24 (2004), www.fas.org/sgp/crs/RL31845.pdf (accessed Sept. 23, 2009); UNITED STATES HOUSE OF REPRESENTATIVES COMMITTEE ON GOVERNMENT—MINORITY STAFF SPECIAL INVESTIGATIONS DIVISION, SECRECY IN THE BUSH ADMINISTRATION (2004); David C. Vladeck, *Symposium: Harnessing the Power of Information for the Next Generation of Environmental Law: III.*

precedent.[36] On October 12, 2001, the Attorney General issued a FOIA policy memorandum. The memorandum urged agency personnel to exercise caution in making discretionary disclosures of information protected under FOIA and stated that the Department of Justice would defend agencies' decisions to withhold information under FOIA "unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records."[37] This was a significant change from the standard under the Clinton administration, pursuant to which the Department of Justice would only defend FOIA nondisclosures where the agency could reasonably foresee harm to a party protected by the exemption in disclosing the information.[38] Federal agencies had already removed information from Web sites in the months immediately following the 9/11 attacks.[39] Thousands more documents were removed from federal government Web sites after the White House Chief of Staff issued a March 2002 memorandum instructing federal agencies to review government information not only involving weapons of mass destruction, but also "other information that could be misused to harm the security of our nation and the safety of our people."[40] In fact, within a year of the 9/11 attacks, 13 federal agencies and 3 state Web sites had blocked access to previously available information.[41] The Bush administration also issued a memorandum instructing federal agencies to process FOIA requests for sensitive information in accordance with the Ashcroft Memorandum, that is, looking for all applicable exemptions.[42]

On the legislative front, the Homeland Security Act of 2002 (HSA)[43] established two new mandatory exemptions to FOIA. First, under Title II of the HSA, the Critical Infrastructure Information Act of 2002 (CIAA)[44] exempted from FOIA disclosure certain voluntarily submitted information, provided that the disclosure is accompanied by an express written or oral disclosure that it is being made voluntarily in expectation of protection under the CIAA.[45] Second, under Title XVI, the HSA amended the authorizing legislation for the TSA[46] to create an exemption from FOIA for certain information obtained or developed in carrying out security under the Aviation and Transportation Security Act of 2001 (ATSA) or under Chapter 449 of Title 49. Unauthorized disclosures are punishable by criminal fines, imprisonment, or both, as well as by mandatory removal from office or employment.[47]

Although Congress had enacted FOIA exemptions following the 9/11 attacks, the congressional stance on the Bush Administration's "need to know" FOIA enforcement eventually shifted. In the latter part of the second Bush term, Congress enacted the "Openness Promotes Effectiveness in Our National Government Act of 2007."[48] The OPEN Government Act specifically found that FOIA responses should be based on right to know rather than on need to know.[49]

Access and Dissemination of Information: Information Access—Surveying the Current Legal Landscape of Federal Right-to-Know Laws, 86 TEX. L. REV. 1787, 1790 (2008), www.utexas.edu/law/journals/tlr/assets/archive/v86/issue7/vladeck.pdf (accessed Sept. 18, 2009); Guinevere Jobson, *On the Public's Right to Proprietary Data, a Contribution to the SSRC Data Consortium for Media and Communications Policy* 2 (2007), http://programs.ssrc.org/media/dataconsortium/RighttoAccessMemo0607.pdf (accessed Mar. 4, 2009).

[36] Dep't of Air Force v. Rose, 425 U.S. 352, 96 S. Ct. 1592, 48 L. Ed. 2d 11 (1976) (disclosure, not secrecy is dominant objective of FOIA); U.S. Dep't of State v. Ray, 502 U.S. 164, 112 S. Ct. 541, 116 L. Ed. 2d 526 (1991) (FOIA establishes a strong presumption in favor of disclosure).

[37] The Ashcroft Memo, reprinted by the Coalition of Journalists for Open Government, www.cjog.net/background_the_ashcroft_memo.html (accessed July 31, 2009). The memorandum is no longer available on the Department of Justice Web site.

[38] Uhl, *supra* note 22, at 271.

[39] P. STEPHEN GIDIERE III, THE FEDERAL INFORMATION MANUAL: HOW THE GOVERNMENT COLLECTS, MANAGES AND DISCLOSES INFORMATION UNDER FOIA AND OTHER STATUTES 350–51 (2006). Reportedly much of the information was reposted by other groups. Nicholas Bagley, *Benchmarking, Critical Infrastructure Security, and the Regulatory War on Terror*, 43 HARV. J. ON LEGIS. 47, 68 (2006).

[40] Uhl, *supra* note 22, at 272.

[41] *One Year Later: September 11 and the Internet*, Pew Internet & American Life Project, Sept. 5, 2002, at 8–9, www.pewinternet.org/~/media//Files/Reports/2002/PIP_9-11_Report.pdf.pdf (accessed July 31, 2009). *See also* Stephen Gidiere & Jason Forrester, *Balancing Homeland Security and Freedom of Information*, 16 NAT. RESOURCES & ENV'T 139, 140 (2002), discussing removal of information from agency Web sites since September 11, 2001, www.abanet.org/environ/pubs/nre/specissue/gidiereforrester.pdf (accessed March 4, 2009). In addition, these security concerns may have resulted in an apparent reluctance to post crisis communications or emergency management plans. COMMITTEE ON THE ROLE OF PUBLIC TRANSPORTATION IN EMERGENCY EVACUATION, THE ROLE OF TRANSIT IN EMERGENCY EVACUATION 82 (Transportation Research Board Special Report 294, 2008), http://onlinepubs.trb.org/Onlinepubs/sr/sr294.pdf.

[42] Uhl, *supra* note 22, at 274.

[43] Pub. L. No. 107-296, 16 Stat. 2135, Nov. 25, 2002. For a discussion of legislative history and competing policy arguments, *see* JOHN D. MOTEFF, CRITICAL INFRASTRUCTURE INFORMATION DISCLOSURE AND HOMELAND SECURITY, CRS Report to Congress, RL31547 (2003), www.fas.org/irp/crs/RL31547.pdf (accessed Oct. 9, 2009).

[44] Pub. L. No. 107-296, 16 Stat. 2135, Nov. 25, 2002, Subtitle B—Critical Infrastructure Information (6 U.S.C. § 131–134).

[45] *Id.* § 214(a)(2), codified as 49 U.S.C. § 133(a)(2).

[46] Section 101 of the Aviation and Transportation Security Act (ATSA), Pub. L. No. 107-71, 115 Stat. 597, Nov. 19, 2001, codified as 49 U.S.C. § 114.

[47] Critical Infrastructure Information Act, § 214(f), codified as 6 U.S.C. § 133(f); 6 C.F.R. § 29.9(d). *See* II.B.1, *Federal Legislation*, *infra* this digest.

[48] Pub. L. No. 110-175, 121 Stat. 2524-2531, Dec. 31, 2007.

[49] *See* Vladeck, *supra* note 35, at 1819–21.

Critics of the trend to increasing secrecy have argued that unnecessary restrictions on public access to information violates fundamental public policy principles of open government. In particular, application of the SSI designation has been seen as limiting citizen access to public safety information.[50]

The Obama administration appears to be moving back toward disclosure, with the President issuing an executive order on FOIA on January 21, 2009, stating that the presumption is toward disclosure,[51] and the Attorney General following up with a memorandum to all department and agency heads reminding them that the presumption is to openness, even where the law allows nondisclosure.[52] The Attorney General's March 19, 2009, memorandum specifically rescinded the Attorney General's Memorandum of October 21, 2001, which had in effect encouraged a presumption of nondisclosure. It remains to be seen whether the Obama administration's formal position on FOIA will have any effect on its interpretation of SSI requirements.

Mirroring the trend at the federal level, in the wake of the 9/11 attacks, many states have added security exemptions to their public disclosure laws,[53] although apparently more on the theory that secrecy will increase security than in response to suspicious requests for information.[54] According to an Associated Press analysis of state laws nationwide, of the more than 1,000 laws that have been passed by state legislatures to change access to information, more than twice as many of the measures further restrict access to information than make more information available.[55] While other concerns such as identify theft and privacy of medical records are also at play, the concerns for security have clearly been a driving force. The scope of some of the exemptions has been criticized as overly broad.[56]

3. Disclosure of Bid/Contract Information

Competitive bidding of publicly-funded contracts for large purchases is generally required under both federal and state law[57] and may be advised even where not required.[58] The competitive bidding process is generally intended to provide reasonable competition, thereby protecting the public against discrimination, cronyism, or waste of public funds, and to ensure optimum public benefits from the contracting process.[59] As a California court noted, because of the purposes of competitive bidding, "the public may have a legitimate and substantial interest in scrutinizing the process leading to the selection of the winning proposal."[60]

Nonetheless, information may be kept confidential for competitive purposes of the public agency until the bid/contract is awarded. Federal law prohibits disclosing bid or proposal information before the actual award,[61] and state or local law may contain similar provisions. Certain contract information must also be withheld after award. For example, under the Los Angeles Administrative Code, the contents of proposals must be secured during the negotiations process so that proposers do not obtain pricing and other information about the competing bids during the negotiations process. Such information is not disclosed until an award recommendation is made.[62] It can be argued that by postponing disclosure until after the award recommendation but before the final award, the public can scrutinize the award decision in full and in time to provide input to the decision-makers, thereby balancing the need to know with the need to keep information confidential.[63]

Of course, even once the contract is awarded, some proposal information may be protected from disclosure. Traditionally, competitive information has been the primary concern in this context, but now confidentiality concerns extend to security issues.

---

[50] *E.g.,* Feb. 20, 2007, Comments of the Coalition of Journalists for Open Government to TSA NPRM on Rail Transportation Security, Docket No. TSA-2006-26514, www.cjog.net/documents/TSA_Regulations_Comments.pdf (accessed Feb. 28, 2009); *Looking for Sunshine: Protecting Your Right to Know*, League of Women Voters, Jan. 2006, www.lwv.org/Content/ContentGroups/Projects/OpennessinGovernment/40404_LWV_LoRes.pdf (accessed Sept. 29, 2009).

[51] Memorandum of Jan. 21, 2009—Freedom of Information Act, 74 Fed. Reg. 4683, Jan. 26, 2009, http://edocket.access.gpo.gov/2009/pdf/E9-1773.pdf.

[52] Office of the Attorney General, Memorandum for Heads of Executive Departments and Agencies, Mar. 19, 2009, www.usdoj.gov/ag/foia-memo-march2009.pdf.

[53] DOUGLAS F. GANSLER, REPORT OF THE OFFICE OF ATTORNEY GENERAL ON THE PUBLIC SECURITY EXCEPTION OF THE PUBLIC INFORMATION ACT, App. B (2007), http://www.oag.state.md.us/Opengov/PIA_public_security_exemption_report.pdf. *See* App. C: Exemptions to State Public Records/Freedom of Information Laws, *infra* this digest.

[54] Beth Wade, *Security Through Secrecy*, GOVERNMENT SECURITY MAGAZINE, Nov. 1, 2003, http://govtsecurity.com/mag/security_secrecy/index.html (accessed Feb. 26, 2009).

[55] Tanner, *supra* note 20.

[56] Wade, *supra* note 54.

[57] *E.g.*, OR. REV. STAT. 279C.335, Competitive bidding; exceptions; exemptions, www.leg.state.or.us/ors/279c.html. *See generally* KEVIN M. SHEYS & ROBERT L. GUNTER, REQUIREMENTS THAT IMPACT THE ACQUISITION OF CAPITAL-INTENSIVE LONG-LEAD ITEMS, RIGHTS OF WAY, AND LAND FOR TRANSIT (Transit Cooperative Research Program Legal Research Digest No. 6, 1996).

[58] *E.g.,* [Pennsylvania] Governor's Center for Local Government Services, Purchasing Handbook, downloading available at http://www.newpa.com/get-local-gov-support/publications/index.aspx .

[59] Jennifer Jo Snider Smith, *Competition and Transparency: What Works for Public Procurement Reform.* 38 PUB. CONT. L.J. 114 (2008), noting the importance of FOIA in providing oversight of government contracting.

[60] Michaelis v. Sup. Ct. of Los Angeles County, 38 Cal. 4th 1065, 136 P.3d 194, 44 Cal. Rptr. 3d 663, 668 (2006) (citation omitted).

[61] 41 U.S.C. §§ 253b(f)(4), 253b(m), 423(a).

[62] Michaelis, 44 Cal. Rptr. 3d at 666, citing § 10.15(f)(6) of the Los Angeles Administrative Code.

[63] *See* Michaelis, 44 Cal. Rptr. 3d 663, 38 Cal. 4th 1065, 136 P.3d 194 (Cal. 2006).

A variety of contracts may cover security information. These include contracts to prepare employee manuals and training materials that cover security responses, conduct vulnerability assessments,[64] and prepare or evaluate emergency response plans.[65] In addition, some contracts that do not directly cover security projects may require contractors to access system design documents that constitute SSI/restricted security information:

> Visual and textual architectural and engineering data are vital to understanding the core operations and structural components of transportation infrastructure. This information may include information such as building or structure plans, schematic drawings and diagrams, security system plans, and threat analyses related to the design or security of critical infrastructure—all of which may be of interest to terrorists and could be dangerously misused by someone intending to cause harm to the system or its users, employees, or the general public.... [D]esign documents are often copied and distributed for use by architects, contractors, subcontractors, inspectors, third-party reviewers, and others—all of whom need access to blueprints, engineering schematics, and other technical documents to be able to safely and effectively fulfill their responsibilities.[66]

The FTA Security and Emergency Preparedness Planning Guide defines sensitive information as "any information that would allow a malicious actor to select, or gain information about, a target without the need to physically access it."[67]

It is important that agencies correctly characterize information: As discussed in this report, significant efforts are required to adequately protect designated security information, particularly SSI. Therefore, attempting to withhold nonsensitive information may impair efforts to withhold truly sensitive information.[68]

The range of persons who may request information about requests for proposals or awarded contracts includes contractors, subcontractors, reporters, competitors, citizens/activists, and persons with no legitimate need for the requested information.[69] For security purposes, the final category presents the greatest immediate danger, although any recipient of information could make further disclosure that could have security implications. In any case, state law may not allow the record custodian to inquire as to the identity of the requestor and/or the purpose for which the information is requested.[70]

There are several sources that can make unauthorized disclosures of security information. Agency employees may inadvertently or purposely make unauthorized disclosures. Contractors who have received security information, whether authorized or unauthorized, may make unauthorized disclosures, whether intentionally or from ignorance about their nondisclosure responsibilities. Subcontractors pose the same danger. And once an unauthorized disclosure has been made, each recipi-

---

[64] *E.g.,* Use of contractors in conducting rail security assessments: U.S. GOV'T ACCOUNTABILITY OFFICE, ENHANCED FEDERAL LEADERSHIP NEEDED TO PRIORITIZE AND GUIDE SECURITY EFFORTS 45 (2005), www.gao.gov/new.items/d05851.pdf (accessed Mar. 31, 2009).

[65] *See* Use of Funds, § 1406(b), Pub. L. No. 110-53, 121 Stat. 405–407, 6 U.S.C. § 1135(b). *E.g.*, Connecticut Commuter Rail Security and Emergency Preparedness Planning Study: Legal Notice—Request for Letters of Interest—CSO Solicitation No. 2059, www.das.state.ct.us/rfpdoc/DOT08/bids/2059.pdf (accessed Oct. 1, 2009). There has been some controversy to keeping emergency response plans confidential because of public right to know and ability to respond to threats. *See* Comments of the Silha Center for the Study of Media Ethics and Law on TSA Interim Final Rule on Protection of Sensitive Security Information, July 16, 2004, http://www.silha.umn.edu/assets/pdf/silhacenterssicomments.pdf ; Uhl, *supra* note 22, at 304–5. TRB's Committee on the Role of Public Transportation in Emergency Evacuation recommends making sanitized versions of emergency evacuation plans public:

> The committee believes that the public should be informed about area emergency evacuation plans and how transit will be deployed in an emergency. An informed public, particularly special-needs populations, is critical to preparedness in an emergency incident. However, sensitive operational details should be excluded from emergency planning documents and only "sanitized" versions made publicly available. FEMA could provide a template for suitable presentation formats as part of its guidance to state, local, and tribal governments.

COMMITTEE ON THE ROLE OF PUBLIC TRANSPORTATION IN EMERGENCY EVACUATION, THE ROLE OF TRANSIT IN EMERGENCY EVACUATION 82, Transportation Research Board Special Report 294 (2008), http://onlinepubs.trb.org/Onlinepubs/sr/sr294.pdf.

[66] TRANSTECH MANAGEMENT, INC., *supra* note 1, at 3–4.

[67] BALOG, BOYD, & CATON, *supra* note 1, at 93.

[68] TRANSTECH MANAGEMENT, INC., *supra* note 1, at 3.

[69] Coalition of Journalists for Open Government, *An Opportunity Lost: Part I, An In-Depth Analysis of FOIA Performance From 1998 to 2007* (July 3, 2008), accessed Feb. 28, 2009, at www.cjog.net/documents/Part_1_2007_FOIA_Report.pdf; Society of Professional Journalists, *Frequent Filers: Businesses Make FOIA Their Business*, July 3, 2006, www.spj.org/rrr.asp?ref=31&t=foia (accessed Feb. 26, 2009). *See* II.A.1, *Overview of FOIA*, *infra* this digest.

[70] *E.g.*, Hawaii requires that requested information not subject to disclosure exceptions be made available to any person requesting it. HAW. REV. STAT. § 92F-11(b). In most circumstances anonymity is allowed. Water Service Consumption Data, OIP Op. Ltr. No. 90-29 (Oct. 5, 1990), http://state.hi.us/oip/opinionletters/opinion%2090-29.pdf. Maryland: Superintendent v. Henschen, 279 Md. 468, 473, 369 A.2d 588, 561 (1977) (Maryland statute affords general right of access to any person, without need to show grievance or interest); New Mexico: § 14-2-8(C), N.M. STAT. ANN. 1978 (requesters shall not be required to state their reasons for requesting the records, although they must provide identifying information), www.conwaygreene.com/nmsu/lpext.dll?f=templates&fn=main-h.htm&2.0; North Carolina: § 132[ ]6(b) (individual requesting information not required to disclose reason for inquiry), www.ncleg.net/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_132.html; Texas: A & T Consultants Inc. v. Sharp, 904 S.W.2d 668, 676 (Tex. 1995) (government cannot look at the motives of requester of information); Washington: Livingston v. Cedeno, 164 Wash. 2d 46186 P.3d 1055, 1058 (Wash. 2008) (en banc) (state agency must respond to all public disclosure requests without regard to requester's status or motivation).

ent poses the danger of further unauthorized disclosures.

II. FEDERAL LEGAL ISSUES

A number of federal statutes and regulations govern requirements for disclosing information to the public, safeguarding information from disclosure, and maintaining public records. Such statutes include FOIA and a variety of laws—primarily enacted post-9/11—that cover Critical Infrastructure Information (CII) and SSI. Also covered are laws the requirements of which will require government agencies to generate security information that could be considered CII or SSI.

This section discusses these federal requirements and their importance to transit agencies in managing security information in procurement documents. The section also addresses guidance that may be relevant to such management, including FTA's guidance concerning SSI.

A. FOIA[71]

FOIA applies only to the federal government.[72] It does not create a right of access to records held by state or local government agencies[73] or municipal entities.[74] However, if state or local agency records, such as procurement documents, come into the possession and/or control[75] of a federal agency, those records could be considered federal records for purposes of FOIA.[76] In addition, despite the lack of direct applicability, many states model their open records statutes on the federal statute.[77] Accordingly the rationales of court decisions and guidance for determining whether to disclose information under FOIA are considered persuasive by some state courts[78] and thus relevant to transit agencies' understanding of their disclosure obligations.

1. Overview of FOIA

As the Supreme Court noted in one of its seminal FOIA cases: "The basic purpose of FOIA is to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed." [79] FOIA is intended to assist citizens in discovering "what their government is up to."[80] Accordingly, FOIA establishes a fundamental right of access to federal government records, except to the extent that such records are

---

[71] 5 U.S.C. § 552. *See generally* U.S. DEP'T OF JUSTICE, UNITED STATES DEPARTMENT OF JUSTICE GUIDE TO THE FREEDOM OF INFORMATION ACT (2009), www.justice.gov/oip/foia_guide09.htm (accessed Jan. 17, 2010). *See also* GIDIERE III, *supra* note 39. For a discussion of the statute's legislative history, *see, e.g.*, Michael W. Field, *Rhode Island's Access to Public Records Act: An Application Gone Awry*, 8 ROGER WILLIAMS U. L. REV. 293 (2003).

[72] Jobson, *supra* note 35, at 2.

[73] *E.g.,* Dunleavy v. New Jersey, 251 Fed. App'x 80, 83 (3d Cir. 2007) (unpublished disposition) (stating that FOIA does not impose obligations on state agencies); State *ex rel.* Warren v. Warner, 84 Ohio St. 3d 432,704 N.E.2d 1228 (1999); State *ex rel.* Findlay Publishing Co. v. Schroeder, 76 Ohio St. 3d 580, 669 N.E.2d 835, 839 (1996).

[74] U.S. DEP'T OF JUSTICE, supra note 71 (2009), Entities Subject to FOIA, at 29, n.42, www.justice.gov/oip/foia_guide09/procedural-requirements.pdf, citing Nelson v. City of Plano, Case No. 06CV102, docket accessible thru 2007 U.S. LEXIS 34992 (E.D. Tex. May 14, 2007) (dismissing FOIA claims against municipal corporation); Cruz v. Superior Court Judges, Case No. 3:04CV1103(CFD), 2006 US Dist. LEXIS 8628 (D. Conn. Mar. 1, 2006) (municipal police department); Jones v. City of Indianapolis, 216 F.R.D. 440, 443 (S.D. Ind. 2003) (municipal agencies).

[75] *See* McCullough v. FDIC, CA No. 79CV1132, 1980 U.S. Dist. LEXIS 17685, at *6 (D.D.C. July 28, 1980) (concluding that state report transmitted to FDIC remains under control of state and is not agency record under FOIA in light of state confidentiality statute, but that other reports transmitted to agency by state regulatory authorities might be agency records because "it is questionable whether [state authorities] retained control" over them); Teich v. FDA, 751 F. Supp. 243, 248–49 (D.D.C. 1990) (holding that documents submitted to FDA in "'legitimate conduct of its official duties'" are agency records notwithstanding FDA's presubmission review regulation allowing submitters to withdraw their documents from agency's files).

[76] *See* U.S. DEP'T OF JUSTICE, *supra* note 71 (2009), at 35, n.68, www.justice.gov/oip/foia_guide09/procedural-requirements.pdf.

[77] Daniel J. Solove, *Modern Studies in Privacy Law: Notice, Autonomy and Enforcement of Data Privacy Legislation: Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137, 1159 (2002). *See, e.g.*, Woodstock Academy v. FOIC, 181 Conn. 544, 436 A.2d 266 (1980) (appropriate to look to federal act for guidance in interpreting Connecticut FOIA).

[78] *E.g.*, Michaelis, 44 Cal. Rptr. 3d at 671; Fioretti v. Md. State Bd. of Dental Examiners, 351 Md. 66, 716 A. 2d 258 (1998) (FOIA interpretations persuasive in Maryland Public Information Act cases); Educ. Law Ctr. v. N.J. DOE, 966 A.2d 1054, 1060, 198 N.J. 274, 285 (2009) (because of similarity between New Jersey's deliberative process exemption and FOIA Exemption 5, New Jersey courts "have turned to federal deliberative process jurisprudence, where such law chiefly has developed, for guidance in ascertaining the scope of OPRA's deliberative process exemption."); Progressive Animal Welfare Soc'y v. Univ. of Wash., 54 Wash. App. 180, 773 P.2d 114 (1989) (FOIA interpretations may be used to construe Washington Public Disclosure Act); Opinion of Hawaii's Office of Information Practices, OIP Op. Ltr. No. 07-05 (The exceptions to disclosure found in the federal Freedom of Information Act ("FOIA"), on which the UIPA is indirectly based, generally are more specific and apply to specific types of records described in the law, but under the UIPA many of the situations covered by a specific FOIA exception fall under the general umbrella of frustration…. Thus OIP looks to the examples provided by the UIPA's legislative history and to FOIA case law for guidance in determining how the frustration exception applies to particular types of records.), www.state.hi.us/oip/opinionletters/opinion%2007-05.pdf.

[79] Robbins Tire & Rubber Co., 437 U.S. at 242.

[80] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 773, 109 S. Ct. 1468, 1481, 103 L. Ed. 2d 774, 795 (1989).

protected from disclosure by statutory exceptions.[81] FOIA is intended to balance between the public's right to know and the government's need to protect certain information.[82] The statutory language favors disclosure, as does judicial interpretation.[83]

When Congress amended FOIA in 2007, Congress declared that FOIA should be regularly reviewed "in order to determine whether further changes and improvements are necessary to ensure that the Government remains open and accessible to the American people and is always based not upon the 'need to know' but upon the fundamental 'right to know'."[84] In an effort to ensure that the right to know is enforced, the 2007 amendment added a tracking requirement for FOIA requests.[85]

Two subsections of FOIA provide for automatic availability of certain government records,[86] while a third governs requests for information.[87] For information to be disclosable pursuant to a FOIA request, it must be contained in what is an agency record under FOIA, which includes electronic formats.[88]

Subsection (b) of FOIA contains nine exemptions. The exemptions are to be construed narrowly.[89] The exemptions are generally discretionary rather than mandatory,[90] although the Department of Justice notes that it is not appropriate for agencies to make discretionary disclosure of information that comes under Exemption 3.[91] Applicability of the exemptions does not depend on the identity of the requestor nor the purpose for which the information is requested.[92] To facilitate meaningful review of assertions of exemptions from FOIA, when an agency withholds information under one of the nine exemptions and litigation ensues, the agency must prepare an index describing the withheld documents and explaining why those documents fall under the exemptions asserted.[93] Such an index is commonly referred to as a Vaughn index,[94] in reference to *Vaughn v. Rosen*,[95] the case that first articulated the need for the index. The justification for withholding should be relatively detailed.[96]

Four of the nine exemptions have particular applicability to protection of security information in the context of procurement:

- Exemption 2:[97] records that relate solely to the internal personnel rules and practices of an agency.
- Exemption 3:[98] information that is specifically exempted from disclosure by another statute.
- Exemption 4:[99] trade secrets/commercial or financial information.
- Exemption 5:[100] certain inter-agency or intra-agency analyses or recommendations.

Exemption 2.—This exemption has been interpreted to cover relatively trivial internal matters ("low 2") and matters the disclosure of which would help the recipient

[81] John Doe Agency v. John Doe Corp., 493 U.S. 146, 151–52, 110 S. Ct. 471, 474, 107 L. Ed. 2d 462, 470 (1989).

[82] *Id*. at 152.

[83] Rose, 425 U.S. at 366 (1976) (holding that "limited exemptions do not obscure the basic policy that disclosure, not secrecy, is the dominant objective of the Act"); Alirez v. N.L.R.B., 676 F.2d 423, 425 (10th Cir. 1982); Lion Raisins v. U.S. Dep't of Agriculture, 354 F.3d 1072, 1079 (9th Cir. 2004). *See* I.C.1, *Disclosing Public Records, supra* this digest.

[84] Section 2(6), Openness Promotes Effectiveness in Our National Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524, Dec. 31, 2007.

[85] Section 7 of Pub. L. No. 110-175 (Dec. 31, 2007), amending 5 U.S.C.§ 552(a) by adding paragraph (7). *See* U.S. DEP'T OF JUSTICE, *supra* note 71, at 26.

[86] 5 U.S.C. § 552(a)(1), (a)(2) (2006), amended by OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524, Dec. 31, 2007.

[87] *Id.* § 552(a)(3) (2006).

[88] *Id.* § 552(f)(2)(A) (2006).

[89] *E.g.*, Lion Raisons, 354 F.3d at 1079.

[90] Chrysler Corp. v. Brown, 441 U.S. 281, 293, 91 S. Ct. 1705, 1713, 60 L. Ed. 2d 208, 219 (1979). Attorney General Holder's FOIA guidelines encourage agencies to make discretionary disclosures. Attorney General Holder's Memorandum for Heads of Executive Departments and Agencies Concerning the Freedom of Information Act (Mar. 19, 2009), http://www.usdoj.gov/ag/foia-memo-march2009.pdf (accessed Aug. 16, 2009).

[91] U.S. DEP'T OF JUSTICE, *supra* note 71, at 688, www.justice.gov/oip/foia_guide09/disclosure-waiver.pdf.

[92] *Id.* at 40–46, www.justice.gov/oip/foia_guide09/procedural-requirements.pdf.

[93] Vaughn v. Rosen, 484 F.2d 820, 827–28, 157 U.S. App. D.C. 340 (D.C. Cir. 1973).

[94] *E.g.*, Larson v. Dep't of State, 565 F.3d 857, 385 U.S. App. D.C. 394 (D.C. Cir. 2009). State courts may also require preparation of a Vaughn index under state public records acts. *E.g.*, Farley v. Worley, 215 W.Va. 412, 599 S.E.2d 835 (2004).

[95] 484 F.2d 820, 827–28, 157 U.S. App. D.C. 340 (D.C. Cir. 1973).

[96] Mead Data Central, Inc. v. U.S. Dep't of Air Force, 566 F.2d 242, 251, 184 U.S. App. D.C. 350 (D.C. Cir. 1977).

[97] 5 U.S.C. § 552(b)(2). *See* U.S. DEP'T OF JUSTICE, *supra* note 71, Exemption 2, http://www.justice.gov/oip/foia_guide09/exemption2.pdf .

[98] 5 U.S.C. § 552(b)(3). *See* U.S. DEP'T OF JUSTICE, *supra* note 71, Exemption 3, http://www.justice.gov/oip/foia_guide09/exemption3.pdf; STEVENS & TATELMAN, *supra* note 34, at CRS-1. www.fas.org/sgp/crs/secrecy/RL33670.pdf, at CRS-6–CRS-9; Department of Justice, Agencies Rely on Wide Range of Exemption 3 Statutes, FOIA Post, www.usdoj.gov/oip/foiapost/2003foiapost41.htm`` (accessed Apr. 1, 2009).

[99] 5 U.S.C. § 552(b)(4). *See* U.S. DEP'T OF JUSTICE, *supra* note 71, Exemption 4, http://www.justice.gov/oip/foia_guide09/exemption4.pdf.

[100] 5 U.S.C. § 552(b)(5). *See* U.S. DEP'T OF JUSTICE, *supra* note 71, Exemption 5, http://www.justice.gov/oip/foia_guide09/exemption5.pdf.

to circumvent a legal requirement ("high 2").[101] The latter category is relevant to security information. The Justice Department, following the rule in the D.C. Circuit, interprets Exemption 2 as requiring the information to be predominantly internal.[102] The D.C. Circuit's case adopting the "predominantly internal" standard[103] is widely cited[104] and has been explicitly adopted by the Ninth Circuit.[105] The "high 2" standard then requires that the disclosure of the requested information would have to significantly risk the circumvention of legal requirements.[106] The legal requirement to be circumvented need not relate to criminal matters.[107] The assertion of a "high 2" exemption requires the agency to specifically describe the potential harm from disclosure.[108] The agency bears the burden of establishing that disclosure poses a significant risk of allowing recipients to circumvent agency regulations.[109] For example, the Connecticut District Court addressed the need for specificity in asserting a "high 2" exemption:

> The Court is not willing to accept the agency's word that documents are predominantly internal or that if disclosed, the document would reveal ongoing law enforcement techniques and risk circumvention of the law. Instead, on a motion for summary judgment, it is DHS's responsibility to demonstrate that it has properly withheld documents by providing the Court and Plaintiffs with reasonably detailed descriptions of the documents and with specific, particularized explanations regarding the reasons for withholding each portion of the documents. It does not suffice to give a few examples, as DHS has done.[110]

Vulnerability assessments have been withheld under Exemption 2.[111] Although the practice of asserting Exemption 2 to protect vulnerability assessments[112] predates the enactment of more specific exemptions related to SSI, discussed *infra*, Exemption 2 is still considered relevant for security information.[113]

Exemption 3.—This exemption allows an agency to withhold information prohibited from disclosure under another federal statute, provided that "such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld."[114] This proviso was added to FOIA in 1976 to overrule the Supreme Court's decision in *Administrator, FAA v. Robertson*,[115] which had allowed statutes providing administrative discretion to withhold information to be the basis for Exemption 3 withholdings.[116]

Official disclosure of information waives Exemption 3, but the mere fact that information is in the public domain does not. Moreover, the official disclosure must be specific to constitute a waiver of the ability to claim Exemption 3 for the documents in question.[117] Failure to adhere to the agency's own regulations regarding circulation of internal agency documents may be sufficient to support a finding of waiver,[118] as is, under certain circumstances, agency carelessness in allowing access to documents.[119]

When an agency's decision to withhold documents is challenged, the court must review the documents in question *de novo* to determine the applicability of any exemptions asserted.[120] An Exemption 3 review is a two-

[101] *See, e.g.*, Schiller v. NLRB, 964 F.2d 1205, 1207, 296 U.S. App. D.C. 84 (D.C. Cir. 1992); Judicial Watch, Inc. v. U.S. Secret Service, 579 F. Supp. 2d 182, 186 (D.D.C. 2008).

[102] U.S. DEP'T OF JUSTICE, *supra* note 71, at 189, n.63, *citing* Schreibman v. U.S. Dep't of Commerce, 785 F. Supp. 164, 166 (D.D.C. 1991) (protecting vulnerability assessment of agency's computer security plan); Dorsett v. U.S. Dep't of the Treasury, 307 F. Supp. 2d 28, 36–37 (D.D.C. 2004) (concluding that Secret Service document used to "analyze and profile factual information concerning individuals" who may constitute threat to Secret Service protectees met "predominantly internal" standard); Schwarz v. U.S. Dep't of Treasury, 131 F. Supp. 2d 142, 150 (D.D.C. 2000) (finding "the threat potential to individuals protected by the Secret Service" to be exempt from disclosure under both Exemptions 2 and 7(E)); Voinche v. FBI, 940 F. Supp. 323, 328–29 (D.D.C. 1996) (protecting as "predominantly internal" information relating to security of Supreme Court building and Supreme Court Justices), www.usdoj.gov/oip/foia_guide07/exemption2.pdf.

[103] Crooker v. Bureau of Alcohol, Tobacco & Firearms, 670 F.2d 1051, 1072–74, 216 U.S. App. D.C. 232 (D.C. Cir. 1981) (en banc). Crooker provides an exhaustive analysis of Exemption 2.

[104] *E.g.*, Kaganove v. E.P.A., 856 F.2d 884 (7th Cir. 1988); El Badrawi v. Dep't of Homeland Sec., 583 F. Supp. 2d 285, 316 (D. Conn. 2008).

[105] Milner v. U.S. Dep't of Navy, 575 F.3d 959 (9th Cir. 2009).

[106] Stolt-Nielsen Transp. Group Ltd. v. United States, 534 F.3d 728, 732 (D.C. Cir. 2008).

[107] U.S. DEP'T OF JUSTICE, *supra* note 71, at 191–201, http://www.justice.gov/oip/foia_guide09/exemption2.pdf.

[108] *Id.* at 205, http://www.justice.gov/oip/foia_guide09/exemption2.pdf.

[109] Crooker, 670 F.2d at 1074; El Badrawi, 583 F. Supp. 2d at 316.

[110] Lowenstein v. Dep't of Homeland Sec., 603 F. Supp. 2d 354, 360 (D. Conn. 2009).

[111] TRANSTECH MANAGEMENT, INC., *supra* note 1, at 7.

[112] FOIA Update, Vol. X, No. 3, at 3–4 (OIP Guidance: Protecting Vulnerability Assessments Through Application of Exemption Two), www.usdoj.gov/oip/foia_updates/Vol_X_3/page3.html.

[113] U.S. DEP'T OF JUSTICE, *supra* note 71, at 203–06, http://www.justice.gov/oip/foia_guide09/exemption2.pdf.

[114] 5 U.S.C. § 552(b)(3); Irons & Sears v. Dann, 606 F.2d 1215, 1220, 196 U.S. App. D.C. (D.C. Cir. 1979).

[115] 422 U.S. 255, 95 S. Ct. 2140, 45 L. Ed. 2d 164 (1975).

[116] Irons & Sears, 606 F.2d at 1219–20.

[117] American Civil Liberties Union v. Dep't of Defense, 584 F. Supp. 2d 19, 23 (D.D.C. 2008), *citing* Afshar v. Dep't of State, 702 F.2d 1125, 1130, 226 U.S. App. D.C. 388 (D.C. Cir. 1983); Pub. Citizen v. Dep't of State, 11 F.3d 198, 201, 304 U.S. D.C. 154 (D.C. Cir. 1993).

[118] Shermco Indus. v. Secretary of the Air Force, 613 F.2d 1314, 1320 (5th Cir. 1980).

[119] Goodrich v. EPA, 593 F. Supp. 2d 184, 192 (D.D.C. 2009).

[120] 5 U.S.C. § 552(a)(4)(B).

part process: first the court determines whether the statute relied upon falls within the ambit of Exemption 3, then it determines whether the information at issue falls within the scope of the statute relied upon.[121] Both prongs must be satisfied for Exemption 3 to form a basis for withholding requested information.

Exemption 4.—While Exemption 4 protects confidential information, FOIA does not define the term "confidential." Courts have held that confidentiality of records may be determined by looking at the legislative purpose of FOIA. The D.C. Circuit has articulated the following standard for information involuntarily disclosed to the government:

> [C]ommercial or financial matter is "confidential" for purposes of the exemption if disclosure of the information is likely to have either of the following effects: (1) to impair the Government's ability to obtain necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained.[122]

National Parks is considered the leading case on Exemption 4. The D.C. Circuit subsequently adopted two modifications to *National Parks* that have not been universally accepted. The first was when the D.C. Circuit accepted the First Circuit's "third prong" analysis allowing the government to withhold information under Exemption 4 if disclosure would damage the efficient execution of the government's statutory responsibilities.[123] The other was when the D.C. Circuit modified its rule to apply the *National Parks* standard to information involuntarily submitted, and to find that financial or commercial information voluntarily submitted is confidential under Exemption 4 "if it is of a kind that would customarily not be released to the public by the person from whom it was obtained."[124] The voluntary submission standard under *Critical Mass* requires that the agency possess the authority to require submission of the information at issue and actually exercise that authority in order for the submission not to be voluntary. The submitter's mistaken belief that the agency has such authority does not make the submission involuntary.[125] No other court of appeal has adopted the *Critical Mass* distinction between voluntary and involuntarily submitted information, although some district courts have done so.[126]

Competitors may invoke Exemption 4 in filing "reverse" FOIA actions.[127] For example, ERG Transit Systems (USA), Inc. (ERG) sued the Washington Metropolitan Area Transit Authority (WMATA) to prevent WMATA from releasing ERG's requests for change orders and for an equitable adjustment on a WMATA contract to its competitor, Cubic Transportation Systems, Inc., under WMATA's Public Access to Records Policy. The district court rejected WMATA's argument that because the contract required ERG to submit the documents if it wanted to pursue a change and ERG submitted them to obtain additional compensation, the submission was involuntary. Such a finding would have held the information to a standard of confidentiality that it did not meet. Instead, the court held that information submitted to get a contract adjustment was voluntarily submitted and therefore subject to the more lenient standard of what constitutes confidential information: "of a kind that would customarily not be released to the public by the person from whom it was obtained."[128]

Exemption 5.—This exemption, which has been construed to protect information that would be privileged in the civil discovery context, has been interpreted to incorporate three privileges: deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege.[129] The attorney-client privilege, which could be asserted in the contract negotiation context, will only apply if the communication is based on confidential information provided by the client. The privilege does not apply if the information has been shared with a third party, at the time of the communication or later.[130] However, generally speaking, of the available Exemption 5 privileges, the deliberative process privilege is most likely to be relevant for protection of contract documents. This privilege has clearly been held to be relevant to agency discussions of contract positions.[131] In terms of protecting the agency's deliberative process, documents must be both deliberative and predecisional to be covered by Exemption 5. After the fact explanatory communications are not covered by Exemption 5, nor are predecisional but nondeliberative documents.[132] The deliberative process privilege will

[121] Cent. Intelligence Agency v. Sims, 471 U.S. 159, 167, 105 S. Ct. 1881, 1887, 85 L. Ed. 2d 173, 182 (1985); Minier v. Central Intelligence Agency, 88 F.3d 796, 801 (9th Cir. 1996).

[122] Nat'l Parks and Conservation Ass'n v. Morton, 498 F.2d 765, 770, 162 U.S. App. D.C. 223 (D.C. Cir. 1974) (footnote omitted).

[123] GIDIERE III, *supra* note 39, at 240–41, citing 9 to 5 Organization for Women Office Workers v. Bd. of Governors of the Fed. Reserve Sys., 721 F.2d 1 (1st Cir. 1983) and Critical Mass Energy Project v. Nuclear Regulatory Comm., 830 F.2d 278, 286, 265 U.S. App. D.C. 130 (D.C. Cir. 1987).

[124] Critical Mass Energy Proj. v. Nuclear Regulatory Comm., 975 F.2d 879, 298 U.S. App. D.C. 8 (D.C. Cir. 1992).

[125] GIDIERE III, *supra* note 39, at 242.

[126] *Id*. at 241–42.

[127] *See* U.S. DEP'T OF JUSTICE, *supra* note 71, at 863–80, http://www.justice.gov/oip/foia_guide09/reverse-foia.pdf.

[128] ERG Transit Systems (USA), Inc. v. Wash. Metro. Area Transit Auth., 593 F. Supp. 2d 249, 253 (D.D.C. 2009).

[129] Nat'l Labor Relations Bd. v. Sears, Roebuck Co., 421 U.S. 132, 149, 95 S. Ct. 1504, 1515, 44 L. Ed. 2d 29, 46–47 (1975).

[130] Mead Data v. U.S. Air Force, 566 F.2d 242, 253–54 (1977).

[131] *Id*. at 257, where the court stated: "Discussions among agency personnel about the relative merits of various positions which might be adopted in contract negotiations are as much a part of the deliberative process as the actual recommendations and advice which are agreed upon. As such they are equally protected from disclosure by exemption five."

[132] Sears, Roebuck, 421 U.S. at 151–52; Tax Analysts v. IRS, 117 F.3d 607, 616, 326 U.S. App. D.C. 53 (D.C. Cir. 1997); Con-

apply "as long as a document is generated as part of such a continuing process of agency decision-making."[133] Key to determining whether the communication is deliberative is whether "disclosure of the information would 'discourage candid discussion within the agency.'"[134]

Segregability.—Part of the court's responsibility in reviewing withheld documents is to make a finding regarding the segregability of any nonexempt material:[135] that is whether the material that is not properly subject to exemption can be segregated from the properly exempt material and released, rather than withholding the entire document based on the exempt status of a portion of the document. The judicial concept of segregability[136] was codified by the 1974 amendments to FOIA.[137] The concept of segregability applies to SSI as well as to other security information.[138]

Information Publicly Available.[139]—Whether prior disclosures of information constitute a waiver of an otherwise applicable exemption is fact specific.[140] It depends on the circumstances of the prior disclosure (manner of prior disclosure and form and completeness of the information already disclosed), and on the harm to be caused by the release based on the exemption asserted.[141] The requester of the information bears the burden of demonstrating that the information is publicly available. Prior release of documents may waive the release of the same documents, but not similar unreleased documents.[142] However, the release of similar information in the past may support a finding that the exemption asserted does not in fact apply.[143] Unofficial disclosure or leaks may not be sufficient to constitute a waiver,[144] and, generally speaking, mistaken releases of otherwise exempt information do not waive the applicable FOIA exemption.[145]

Mosaic Effect.[146]—Agencies may be able to withhold information that is not valuable in and of itself but that when combined with other available information may be damaging to disclose. This effect applies to Exemption 4 and could apply in the context of security information.

Agency Implementation.—The DOT has issued regulations governing FOIA requests for DOT. Both DOT and FTA provide guidance on making FOIA requests.[147]

2. Cases Construing FOIA in Transportation Security Context

Both 49 U.S.C. § 114(s) and 49 U.S.C. § 40119(b) relate to nondisclosure of SSI.[148] At least two federal district courts have found both provisions to constitute Exemption 3 statutes.[149]

In *Gordon*, plaintiffs sought information about the TSA's no-fly list. The Federal Bureau of Investigation (FBI) and TSA claimed that requested records were exempt from disclosure pursuant to §§ 114(s) and 40119(b). Citing the prohibitions in the Title 49 provisions, the court held that there was "no dispute that these statutes fall within Exemption 3," the question being rather whether the withheld information fell within the regulations adopted under those statutes.[150] In reviewing the redacted information, the court re-

cepcion v. F.B.I., 606 F. Supp. 2d 14 (D.D.C. 2009); James Madison Project v. C.I.A., 607 F. Supp. 2d 109 (D.D.C. 2009).

[133] Nat'l Ass'n of Home Builders v. Norton, 309 F.3d 26, 39, 353 U.S. App. D.C. 374 (D.C. Cir. 2002) (holding that document is predecisional if it was prepared to assist agency in arriving at decision, rather than supporting decision already made); Elec. Privacy Info. Ctr. v. DHS, 384 F. Supp. 2d 100, 112 (D.D.C. 2005).

[134] Access Reports v. Dep't of Justice, 926 F.2d 1192, 1195, 288 U.S. App. D.C. 319 (D.C. Cir. 1991); Elec. Privacy, 384 F. Supp. 2d at 112.

[135] Nat'l Law Ctr. on Homelessness & Poverty v. U.S. Dep't of Veteran Affairs, 964 F.2d 1210, 296 U.S. App. D.C. 89 (D.C. Cir. 1992); ACLU v. U.S. Dep't of Defense, 584 F. Supp. 2d 23 (D.D.C. 2008).

[136] EPA v. Mink, 410 U.S. 73, 91, 93 S. Ct. 827, 35 L. Ed. 2d 117, 134 (1973).

[137] Pub. L. No. 93-502, 88 Stat. 1561, Nov. 21, 1974. § 2(c), inserted the provision relating to availability of segregable portion of records: "Any reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under this subsection."

[138] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, CLEAR POLICIES AND OVERSIGHT NEEDED FOR DESIGNATION OF SENSITIVE SECURITY INFORMATION 4 (2005), www.gao.gov/new.items/d05677.pdf (accessed Mar. 1, 2009); U.S. GOV'T ACCOUNTABILITY OFFICE, TRANSPORTATION SECURITY ADMINISTRATION'S PROCESSES FOR DESIGNATING AND RELEASING SENSITIVE SECURITY INFORMATION 5 (2007), www.gao.gov/new.items/d08232r.pdf (accessed July 30, 2009).

[139] GIDIERE III, *supra* note 39, at 284.

[140] Mobil Oil Corp. v. Envtl. Protection Agency, 879 F.2d 698, 700 (9th Cir. 1989).

[141] GIDIERE III, *supra* note 39, at 284.

[142] Mobil Oil, 879 F.2d at 700–01.

[143] Army Times Pub. Co. v. Dep't of Air Force, 998 F.2d 1067, 1071, 305 U.S. App. D.C. 432 (D.C. Cir. 1993).

[144] GIDIERE III, *supra* note 39, at 285.

[145] U.S. DEP'T OF JUSTICE, *supra* note 71, at 690–703, www.justice.gov/oip/foia_guide09/disclosure-waiver.pdf. *But see* GIDIERE III, *supra* note 39, at 285 (prior releases due to the agency's error may constitute a waiver).

[146] *See generally* GIDIERE III, *supra* note 39, at 8.13, *Mosaic Effect*.

[147] 49 C.F.R. pt. 7. subpt. C—Availability of Reasonably Described Records Under the Freedom of Information Act, www.access.gpo.gov/nara/cfr/waisidx_08/49cfr7_08.html; DOT's FOIA Reference Guide, www.dot.gov/foia/foiareferenceguide.htm#where; FTA's instructions for FOIA requests, www.fta.dot.gov/about/about_FTA_186.html.

[148] *See* II.B, *Critical Infrastructure Information (CII)/SSI*, *infra* this digest.

[149] Gordon v. FBI, 390 F. Supp. 2d 897, 900 (N.D. Cal. 2004); Gordon v. FBI, 388 F. Supp. 2d 1028 (N.D. Cal. 2005) (cross-motions for summary judgment); Elec. Privacy Info., 384 F. Supp. 2d 110 n.10.

[150] Gordon, 390 F. Supp. 2d at 900.

jected TSA's position that all information within a security directive is SSI, even if that information appears elsewhere.

The *Gordon* court found that simply reciting that information derived from security directives is SSI did not meet defendants' burden of explaining why the information was exempt from disclosure. The court also found that defendants had not met the burden of explaining why innocuous information such as the fact "the Watch lists include persons who pose a threat to aviation" should be withheld.[151] The court held that general statements that the information is SSI do not meet the government's burden. The court ordered the federal defendants to review all of the withheld material to determine whether they believed "in good faith" that the material was in fact exempt and if so to submit a detailed affidavit that explains why particular material was exempt. The court admonished that statements that information is SSI would not meet the government's burden. The court further ordered that any subsequent motion for summary judgment must be accompanied by a certification by government counsel that "counsel has personally reviewed all of the withheld information and in counsel's good faith opinion the withheld material is exempt from disclosure."[152]

Following the court's 2004 order, the TSA submitted a declaration addressing each redaction and explaining specifically why TSA had determined the redaction to be SSI. Upon reviewing the submission, the District Court found that the redacted SSI was appropriately withheld.[153] Although not discussed in the 2004 opinion, Exemption 2 was discussed in the 2005 opinion. The court reviewed whether the information withheld under Exemption 2 would "assist terrorists in circumventing the purpose of the watch lists."[154] The court did not explain specifically why information was correctly withheld, but did find that the FBI had not adequately explained how certain information—the legal basis for detaining someone whose name appears on a watch list—could be used to circumvent agency regulations, and therefore ordered that the FBI release that information.

In *Electronic Privacy Information Center*, the plaintiff sought documents about TSA's attempts to get passenger data from airlines for the Computer Assisted Passenger Prescreening System. In reviewing the defendants' assertion that certain documents were exempt from disclosure pursuant to 49 U.S.C. § 114(s) and 49 U.S.C. § 40119(b), the court noted that to come under Exemption 3, "the statute must 'on its face, exempt matters from disclosure.'"[155] There was no dispute that the statutes provided a basis for asserting Exemption 3.[156] Although the plaintiffs had agreed to exclude documents marked as SSI from the scope of the litigation, the court did require more of a showing than that a document was marked as SSI. The court found that describing a document as constituting selection criteria proposed for aviation screening and marking it as SSI was adequate indication that its disclosure would be detrimental to transportation security, and therefore it was properly withheld; merely marking a document as SSI without further description was not adequate to support the failure to disclose.[157]

3. DOT Use of Exemption 3

As indicated by Parts IV and V of the USDOT FOIA reports for fiscal years 2004–2008, during that time frame agencies within USDOT did cite 49 U.S.C. § 40119 in support of denying FOIA requests. In addition, agencies cited the National Defense Authorization Act of 1997,[158] which prohibits disclosing contract proposals.[159] However, FTA did not cite Exemption 3 at all during that time as the basis for withholding information under FOIA.[160]

4. Release of Security Information

Federal employees who make unauthorized disclosures of SSI may be subject to disciplinary action.[161]

---

[151] *Id*.

[152] *Id*. at 902.

[153] Gordon, 388 F. Supp. 2d at 1028.

[154] *Id*. at 1036.

[155] Elec. Privacy Info, 384 F. Supp. 2d at 109–10, citing Reporters Comm. for Freedom of the Press v. U.S. Dep't of Justice, 816 F.2d 730, 735 (D.C. Cir. 1987).

[156] *Id*. at 110 n.10.

[157] *Id*. at 110.

[158] 41 U.S.C. § 253b(m).

[159] Hornbostel v. Dep't. of Interior, 305 F. Supp. 2d 21 (D.D.C. 2003).

[160] U.S. DEP'T OF TRANSP., FREEDOM OF INFORMATION ACT (FOIA) 2004 ANNUAL REPORT, www.dot.gov/foia/reports/2004annualreport.pdf; U.S. DEP'T OF TRANSP., FREEDOM OF INFORMATION ACT (FOIA) 2005 ANNUAL REPORT, www.dot.gov/foia/reports/2005annualreport.pdf; U.S. DEP'T OF TRANSP., FREEDOM OF INFORMATION ACT (FOIA) 2006 ANNUAL REPORT, www.dot.gov/foia/reports/2006annualreport.pdf; U.S. DEP'T OF TRANSP., FREEDOM OF INFORMATION ACT (FOIA) 2007 ANNUAL REPORT, www.dot.gov/foia/reports/2007annualreport.pdf; U.S. DEP'T OF TRANSP., FREEDOM OF INFORMATION ACT (FOIA) 2008 ANNUAL REPORT, www.dot.gov/foia/reports/2008annualreport.pdf.

[161] 49 C.F.R. § 15.17; MacLean v. Dep't of Homeland Sec., 543 F.3d 1145 (9th Cir. 2008). *Cf.*, Driver Privacy Protection Act penalties: 18 U.S.C. § 2723. The statute is intended to protect the privacy of driver records held by state departments of transportation. State departments of motor vehicles in substantial noncompliance with the statutory requirements for maintaining privacy are subject to fines of up to $5,000 per day for each day of substantial noncompliance, http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc18.wais&start=4193565&SIZE=900&TYPE=TEXT; 18 U.S.C. § 2724 authorizes a private right of action against "[a] person who knowingly obtains, discloses or uses personal information from a motor vehicle record, for a purpose not permitted…, [and makes the person who violates the DPPA] liable to the individual to whom the information pertains…," without any showing that the person to whom the personal information pertains

Even a brief text message with information about air security measures can constitute SSI.[162]

To the extent that information must be kept confidential, agencies need to make sure that both hard copy and electronic systems are secure.

B. Critical Infrastructure Information/Sensitive Security Information

CII is a defined term under federal law. In addition, the Department of Homeland Security (DHS) implementing regulation coined the term "PCII" to apply to specific infrastructure information that is protected under federal law.[163] The information must not only relate to critical infrastructure, but as is discussed *infra*, must meet specific statutory criteria, including being voluntarily submitted to DHS. Thus, information about mass transit infrastructure that is critical to the community in which it is located or to the nation at large because of its interconnectedness with major economic networks (such as the transit system in New York City) is not necessarily protected CII for purposes of the federal statute. However, as the FTA notes, transit agencies "may come in contact with PCII through interaction with the Federal government."[164] While CII, let alone PCII, is likely to be of limited applicability to most transit agencies, particularly in the context of competitive bidding, a basic understanding of CII requirements is relevant. Transit agencies may themselves voluntarily submit information to DHS that, providing it meets statutory requirements described *infra*, will be considered protected CII. Protection of such information applies to DHS, not to the submitting agency, to the extent that the submitting agency uses its own copy of the information and not the validated (and thus protected) CII.[165]

The term SSI has evolved based on aviation security requirements dating back to 1974,[166] and has been extended by USDOT to apply to all modes of transportation.[167] The authorizing legislation for the USDOT and TSA provisions,[168] discussed *infra*, is substantially similar, as are the regulatory provisions themselves.[169] TSA defines SSI as information that is

> obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would—
>
> (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);
>
> (2) Reveal trade secrets or privileged or confidential information obtained from any person; or
>
> (3) Be detrimental to the security of transportation.[170]

Despite the fact that the USDOT provision refers to information the disclosure of which would be "detrimental to transportation safety" rather than "detrimental to transportation security" as under the DHS provision, the USDOT provision is interpreted as governing security issues as well as safety issues.[171] Any security program or security contingency plan "issued, established, required, received, or approved by DOT or DHS" constitutes SSI. Vulnerability assessments that are "directed, created, held, funded, or approved by the DOT [or] DHS, or that will be provided to DOT or DHS in sup-

---

"suffered any adverse effect." Wemhoff v. District of Columbia, 887 A.2d 1004, 1013 (D.C. 2005), *citing* Schmidt v. Multimedia Holdings Corp., 361 F. Supp. 2d 1346, 1348, 1354 (M.D. Fla. 2004).

[162] MacLean, 543 F.3d 1145.

[163] 6 C.F.R. § 29.2.

[164] KEVIN CHANDLER, PAMELA SUTHERLAND, & DONALD ELDREDGE, SENSITIVE SECURITY INFORMATION (SSI): DESIGNATION, MARKINGS, AND CONTROL, RESOURCE DOCUMENT FOR TRANSIT AGENCIES 3 (2009), http://transit-safety.fta.dot.gov/publications/security/FTA%20SSI/Final%20FTA%20SSI%20%28072009%29%20revised.pdf.

[165] DEP'T OF HOMELAND SECURITY, HOW TO SUBMIT CRITICAL INFRASTRUCTURE INFORMATION (CII) FOR PCII PROTECTION, www.dhs.gov/files/programs/gc_1193091627563.shtm (accessed Sept. 2, 2009). *See also* PCII Program FAQ, www.dhs.gov/xlibrary/assets/pcii_faqs.pdf; PCII PROGRAM PROCEDURES MANUAL, www.dhsgov/xlibrary/assets/pcii_program_procedures_manual.pdf.

[166] The Air Transportation Security Act of 1974 (Pub. L. No. 93-366 § 316, 88 Stat. 409 (1974)) authorized the Federal Aviation Administration (FAA) to issue regulations prohibiting disclosure of information developed during research and development that the FAA found would constitute unwarranted invasion of personal privacy, reveal trade secrets or privileged commercial information, or be detrimental to the safety of persons traveling in air transportation. *See* TODD B. TATELMAN, INTERSTATE TRAVEL: CONSTITUTIONAL CHALLENGES TO THE IDENTIFICATION REQUIREMENT AND OTHER TRANSPORTATION SECURITY REGULATIONS, CRS Report for Congress, RL32664 (2004), www.fas.org/sgp/crs/RL32664.pdf, for discussion of history of law governing SSI.

[167] Department of Homeland Security, Transportation Security Administration, Interim Final Rule, *Protection of Sensitive Security Information*, Fed. Reg. 69, No. 96, 28066, May 18, 2004, http://edocket.access.gpo.gov/2004/pdf/04-11142.pdf; CHANDLER, SUTHERLAND & ELDREDGE, *supra* note 164, at 2, http://transit-safety.fta.dot.gov/publications/security/FTA%20SSI/Final%20FTA%20SSI%20%28072009%29%20revised.pdf, at 2.

[168] 49 U.S.C. § 40119(b); 49 U.S.C. § 114(s).

[169] 49 C.F.R. pt. 15; 49 C.F.R. pt. 1520.

[170] 49 C.F.R. § 1520.5(a) *Sensitive security information*. The corollary DOT provision is 49 C.F.R. § 15.5(a) *Sensitive security information*.

[171] CHANDLER, SUTHERLAND & ELDREDGE, *supra* note 164, at 1. *See also* Third Party Contracting Guidance: Notice of Final Circular, 73 Fed. Reg. 56896, 56906 (Sept. 30, 2008):

> FTA has determined that these laws and regulations [49 U.S.C. 40119(b), 49 C.F.R. 15; 49 U.S.C. 14(s), 49 C.F.R. 1520] do apply to public transportation agencies and other FTA recipients that have sensitive security information, such as information related to vulnerability assessments (including any information addressing vulnerabilities or corrective actions) conducted after September 11, 2001, and other information covered by the regulations.

port of a Federal security program" are specifically included in that category.[172] In addition, TSA has issued a Stakeholder Best Practices Quick Reference Guide in which the agency lists a wide range of information the agency deems to constitute SSI.[173]

Managing SSI is more likely to be of concern to transit agencies than is managing CII. A number of federal requirements make it likely that transit agencies will need to comply with Federal SSI requirements, including the following:

- Establishing a National Strategy for Public Transportation Security,[174] including use of public transportation security assessments.
- Establishing a Transportation Security Information Sharing Plan.[175]
- Preparing assessments and plans that will result in security assessments being submitted to DHS for transit agencies at a high risk of attack and for representative samples of non-high-risk transit agencies.[176]

Even where federal requirements are not directly applicable, for example, for vulnerability assessments that are funded locally and not shared with federal agencies and thus do not meet the SSI statutory criteria, transit agencies may have security information that should be protected. Thus, the federal requirements may nonetheless be instructive on issues for transit agencies to consider in adopting their own policies.

Issues that arise concerning SSI designation include maintaining consistency in designating SSI, avoiding the problem of over-designating information as SSI, protecting SSI, reviewing SSI over time to determine whether its confidential status remains justified, and disposing of SSI. For example, DHS has been criticized for asserting overly broad claims for withholding sensitive information.[177] As noted *supra*, in *Gordon,* the federal district court judge rejected the government's assertion that requested material was SSI or otherwise exempt from FOIA, finding rather that withheld material was innocuous and in some instances publicly available.[178]

This section reviews the authorizing legislation for CII and SSI provisions, as well as federal programs, requirements, and guidance related to CII and SSI by relevant agency. The purpose is to clarify the meaning and applicability of these terms and their attendant requirements. This is particularly important since to the extent that information comes within the definition of CII or SSI, that information becomes exempt from state disclosure requirements.[179]

1. Federal Legislation

Several pieces of legislation that passed after the events of 9/11 vested the DHS, TSA, and USDOT with responsibility for administering CII and SSI requirements. The legislation is described below and included in Appendix A. Federal transit legislation that has im-

[172] 49 C.F.R. § 15.5(b)(5); 49 C.F.R. § 1520.5(b)(5).

[173] TRANSP. SECURITY ADMIN., SENSITIVE STAKEHOLDER BEST PRACTICES QUICK REFERENCE GUIDE, included as App. B to Chandler, *supra* note 163. Information listed: security programs and contingency plans; security directives; information circulars; performance specifications; vulnerability assessments; security inspections or investigative information; threat information; security measures; security screening information; security training materials; identifying information of certain transportation security personnel; critical infrastructure asset information; systems security information; confidential business information; research and development; and other information as determined in writing by the TSA Administrator.

[174] Section 1404, Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 401, Aug. 3, 2007, codified at 6 U.S.C. § 1133. Section 1404 (d)(2) references already developed security and strategies: National Infrastructure Protection Plan, www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (accessed Sept. 2, 2009) required by Homeland Security Presidential Directive–7; Executive Order No. 13416: Strengthening Surface Transportation Security, Dec. 5, 2006, Fed. Reg. 71, No. 235, 71033, Dec. 7, 2009, Accessed Sept. 13, 2009, at http://edocket.access.gpo.gov/2006/pdf/06-9619.pdf; the Memorandum of Understanding between DHS and the DOT on Roles and Responsibilities dated Sept. 28, 2004. The sector-specific plan for mass transit is included as Annex C., Mass Transit, in *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan as Input to the National Infrastructure Protection Plan*, May 2007, www.dhs.gov/xlibrary/assets/Transportation_Base_Plan_5_21_07.pdf (accessed Sept. 2, 2009).

[175] Section 1203, Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 383, Aug. 3, 2007, codified at 49 U.S.C. § 114(u).

[176] Section 1405, Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 402, Aug. 3, 2007, codified at 6 U.S.C. § 1134 (National Transit Systems Security Act of 2007 is Title XIV of the public law.)

[177] *E.g.*, Amicus Curiae Brief of Electronic Frontier Foundation, American Association of Law Libraries, American Library Association, Association of Research Libraries, Center for Democracy and Technology, National Security Archive, Project on Government Secrecy of the Federation of American Scientists, and Special Libraries Association on Petition for Writ of Certiorari to the Court of Appeals for the Ninth Circuit, Gilmore v. Gonzalez, www.papersplease.org/gilmore/_dl/20061113/Gilmore%20v.%20Gonzales%20EFF%20amicus.pdf (accessed Oct. 6, 2009).

[178] Eric Lichtblau, *Judge Scolds U.S. Officials Over Barring Jet Travelers*, N.Y. TIMES, June 16, 2004, www.nytimes.com/2004/06/16/politics/16flight.html (accessed Mar. 24, 2009). The government ultimately settled, agreeing to pay attorneys fees. *TSA and FBI Ordered to Pay $200,000 to Settle "No Fly" Lawsuit*, Jan. 24, 2006, www.aclu.org/safefree/general/23926prs20060124.html (accessed Aug. 1, 2009).

[179] *See* Charles Davis, *More Daunting Tests Ahead Pitting "Right To Know" Against "Need To Know,"* FOI Columns, Jan.–Feb. 2004, www.ire.org/foi/janfeb2004.html (accessed Feb. 28, 2009).

plications is referenced in II.B.2, Federal Agencies, *infra*.

Aviation and Transportation Security Act of 2001 (ATSA).[180]—The ATSA transferred civil aviation security responsibilities from the Federal Aviation Administration (FAA) to TSA, including authority to conduct research and development activities related to security.[181] Section 101(e)(3) of the ATSA-modified Section 40119(b) contains a provision requiring nondisclosure of certain safety-related information, by deleting the modifier "air" from "air transportation." DHS has interpreted this change as expanding the scope of the provision to cover all modes of transportation.[182]

Homeland Security Act of 2002 (HSA).[183]—The HSA adopted the USA PATRIOT Act's definition of critical infrastructure: "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[184] The HSA also added a provision transferring TSA's SSI authority and vesting SSI authority in the DOT Secretary.[185]

Critical Infrastructure Information Act of 2002.[186]—The CIIA was included as Title II of the HSA. Section 211(3) defines "critical infrastructure information"; subsection 214(a) of the CIIA protects CII voluntarily submitted to DHS for use regarding "the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose [sic],"[187] provided the information is accompanied by the express statement required under the statute. Such protected CII is exempt from disclosure under FOIA; prohibited from being used for other official purposes except under very limited circumstances; and if shared with state and local governments and agencies, exempt from disclosure under state or local open records requirements. However, the CIIA does not affect any entity's ability to lawfully obtain CII in a manner not covered by subsection (a) and to use such information in any lawful manner. Thus such information that is customarily in the public domain (lawfully, properly, and regularly disclosed generally or broadly to the public) is not protected.[188] DHS may withdraw the protected status if it determines that at the time of submission the information was customarily in the public domain.[189] Federal employees who knowingly disclose protected CII are subject to fine, imprisonment, and job loss.[190] There is no private right of action to enforce the CIIA.[191]

At least one court has held that the CIIA does not apply to submitters of PCII, so that the CIIA does not preempt requests for information made to the submitting agency under state public records acts.[192] The court noted that the CIIA prohibits disclosure of protected CII under state or local public records acts, but only if the protected CII is provided to a state or local government, and interpreted this statutory language as distinguishing between submission of CII and receipt of protected CII for purposes of when a state or local agency may disclose requested information: submitting CII to the federal government does not require the submitting agency to then withhold that information under the state public records law. The court also reviewed the implementing regulations, discussed *infra*, and found that they also support this distinction between submission and receipt of protected CII for purposes of applica-

---

[180] Pub. L. No. 107-71, 115 Stat. 597, Nov. 19, 2001.

[181] 49 U.S.C. § 40119, Security and research and development activities. Section 40119 authorized the FAA to conduct research and development (R&D) activities aimed at protecting

> passengers and property against acts of criminal violence and aircraft piracy. The provision prohibited disclosure of information obtained or developed in carrying out specified security or R&D activities under specified sections of Chapters 445 (Facilities, Personnel, and Research) and 449 (Security) of title 49, provided that the FAA 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 transportation safety.

[182] Department of Homeland Security, Transportation Security Administration, Interim Final Rule, *Protection of Sensitive Security Information*, Fed. Reg. 69, No. 96, 28066, 28068, May 18, 2004.

[183] Pub. L. No. 107-296, 116 Stat. 2135, Nov. 25, 2002.

[184] Section 2(4), *Definitions*, citing § 1016(e) of Pub. L. No. 107–56 (42 U.S.C.§ 5195c(e)).

[185] Section 1601, *Retention of Sensitive Security Information Authority at Department of Transportation*, codified at 49 U.S.C. § 114(s) and 49 U.S.C. § 40119(b)(1).

[186] Tit. II, subtit. B, HSA, Pub. L. No. 107-296, 116 Stat. 2135, Nov. 25, 2002, codified at 6 U.S.C. §§ 131–34. For a critique of the strategy behind the CIIA, including the fact that the FOIA exemptions hamper public oversight, *see* Bagley, *supra* note 39.

[187] Section 214, *Protection of voluntarily shared critical infrastructure information*, codified at 6 U.S.C. § 133; 6 C.F.R. § 29.8. *See* James W. Conrad, Jr., *Protecting Private Security-Related Information from Disclosure by Government Agencies*, 57 ADMIN. L. REV. 715, nn. 80–89 (2005); presented at ABA meeting, Protection of Facility Security Information, Dec. 10, 2004, http://meetings.abanet.org/webupload/commupload/AL316500/newsletterpubs/Info%20protection.pdf (accessed in prepublication form Mar. 4, 2009).

[188] 6 C.F.R. §§ 29.2, 29.5. Part 29 introduces the term "Protected Critical Infrastructure Information, or PCII," which is not a statutorily defined term. The regulation defines PCII as CII that has been validated by DHS as meeting the statutory criteria for protection.

[189] 6 C.F.R. § 29.6(g).

[190] Section 214, *Protection of voluntarily shared critical infrastructure information*, codified at 6 U.S.C. § 133; 6 C.F.R. § 29.9.

[191] Section 215, codified at 6 U.S.C. § 134.

[192] County of Santa Clara v. Superior Court of Santa Clara County, 170 Cal. App. 4th 1301, 89 Cal. Rptr. 3d 374 (Cal. Ct. App. 6th Dist. 2009).

tion of state public records requirements. The court concluded:

> Taken as a whole, this consistent and pervasive regulatory language supports our construction of the relevant provision of the CII Act, 6 United States Code section 133(a)(1)(E)(i). As we interpret that provision, it draws a distinction between the submission of CII and the receipt of PCII. In the hands of the submitter, the nature of the information remains unchanged; in the hands of the governmental recipient, it is protected from disclosure. (footnote omitted)[193]

The court also noted that if the contrary interpretation were correct, then the Geographic Information System (GIS) Basemap at issue in the case could no longer be used by the county for any purpose other than those enumerated under the CIIA. Accordingly, the prohibition under the CIIA against disclosure under the California Public Records Act was held not to apply.

Department of Homeland Security Appropriations Act, 2006.[194]—This Act requires DHS to appoint at least one SSI coordinator in each DHS office that handles SSI to ensure that documents marked as SSI meet the SSI criteria. It requires the Secretary to issue guidance that "includes common but extensive examples of SSI that further define the individual categories of information cited under 49 C.F.R. 1520(b)(1) through (16) and eliminates judgment by covered persons in the application of the SSI marking."[195] The Act also required the Government Accountability Office (GAO) to report on DHS progress in implementing the law's requirements.

Department of Homeland Security Appropriations Act, 2007.[196]—The Act requires DHS to revise its Management Directive (MD) 11056, which establishes DHS policy regarding the recognition, identification, and safeguarding of SSI, as specified in the legislation, and it requires GAO to report on DHS' progress in implementing the law's requirements.[197] The Act also extended the designation of "covered person" to a party in civil litigation who can demonstrate both a substantial need for relevant SSI in preparing the party's case and an undue hardship in obtaining equivalent information by other means, provided that the judge enters an order protecting the SSI from unauthorized disclosure, the party undergoes a threat assessment including criminal background check, and access does not present a risk of harm to the nation. GAO reports that the directive has been revised.[198]

Implementing Recommendations of the 9/11 Commission Act of 2007.[199]—The Act contains several provisions that will require generating information that could be considered to be CII or SSI because of the information being shared with DHS and USDOT for security purposes. These include grant provisions that public transportation agencies implement in part through contracts with private entities. The discussion here of this Act are limited to those provisions that require information generation that might reasonably be expected to result in procurement activity.[200]

As noted, *supra*, Section 1203 requires DHS and USDOT, along with public and private stakeholders, to establish a Transportation Security Information Sharing Plan.[201] Section 1305 requires DHS, in consultation with USDOT, to establish a program to share information about transportation security technology with, *inter alia*, public transportation agencies.[202] Title XIV of the Act, the National Transit Systems Security Act of 2007 (NTSSA), requires DHS to develop and implement the National Strategy for Public Transportation Security. In meeting that requirement, DHS is required to "use established and ongoing public transportation security assessments" and "consult with all relevant stakeholders, including public transportation agen-

---

[193] *Id*. at 1318.

[194] Pub. L. No. 109–90, 119 Stat. 2064, Oct. 18, 2005.

[195] *Id*. Tit. V, § 537, codified at 6 U.S.C. § 114. The provision also required GAO to report on DHS progress in implementing the law's requirements.

[196] Pub. L. No. 109–295, 120 Stat. 1355, Oct. 4, 2006.

[197] *Id*. at § 525. Section 525 requires that MD 11056 be revised to provide as follows:

> (1) That when a lawful request is made to publicly release a document containing information designated as sensitive security information (SSI), the document shall be reviewed in a timely manner to determine whether any information contained in the document meets the criteria for continued SSI protection under applicable law and regulation and shall further provide that all portions that no longer require SSI designation be released, subject to applicable law, including sections 552 and 552a of title 5, United States Code;
>
> (2) That sensitive security information that is three years old and not incorporated in a current transportation security directive, security plan, contingency plan, or information circular; or does not contain current information in one of the following SSI categories: equipment or personnel performance specifications, vulnerability assessments, security inspection or investigative information, threat information, security measures, security screening information, security training materials, identifying information of designated transportation security personnel, critical aviation or maritime infrastructure asset information, systems security information, confidential business information, or research and development information shall be subject to release upon request unless:
>
> (A) the Secretary or his designee makes a written determination that identifies a rational reason why the information must remain SSI; or
>
> (B) such information is otherwise exempt from disclosure under applicable law.

[198] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 138, at 5. Some guidance may be available to transit agencies through FTA or TSA that is not publicly available, and therefore cannot be discussed in this report.

[199] Pub. L. No. 110-53, 121 Stat. 266, Aug. 3, 2007.

[200] *Cf.*, § 1410, Information sharing, codified at 6 U.S.C. § 1139 (requiring public transportation agencies at high risk of terrorist attack to participate in the Information Sharing and Analysis Center for Public Transportation), which does not appear likely to result in procurement activity. *See* V.B.3, *Controls Within the Agency*, *infra* this digest, for a discussion of the NTSSA's requirements for security background checks.

[201] Codified at 49 U.S.C. § 114(u).

[202] Codified at 6 U.S.C. § 1114.

cies."[203] The NTSSA also requires DHS to conduct certain public transportation security assessments. In addition, the Act mandates that DHS require public transportation agencies determined by DHS to be at high risk of terrorist attack to develop comprehensive security plans, with technical assistance provided by DHS. If DHS requires any other public transportation agencies to prepare security plans, DHS must provide technical assistance to those agencies as well. The statute specifies the contents of such security plans, including requiring them to be consistent with security assessments developed by DHS and with the National Strategy for Public Transportation Security. The requirement for developing security assessments or security plans may be recognized by DHS as being met by existing procedures, protocols, and standards of a public transportation agency.[204] Finally, the statute addresses nondisclosure as follows: "Nothing in this section shall be construed as affecting any authority or obligation of a Federal agency to disclose any record or information that the Federal agency obtains from a public transportation agency under any other Federal law."[205]

The security assistance program established under the NTSSA allows both capital and operating use of funding, with all funding to be awarded solely to address items included in a security assessment or to further a security plan.[206] Agencies that receive such funding must develop training programs as specified under the statute.[207]

The NTSSA also contains a provision covering security background checks of public transportation employees and contractors.[208] The provision sets parameters for DHS guidance on background checks and requires DHS regulation on background checks to provide a redress process and prohibit specified adverse actions based on the background checks. In addition, the statute and its implementing regulation prohibit public transportation agencies from knowingly making false statements to employees concerning security background checks.[209]

---

[203] Section 1404, National Strategy for Public Transportation Security, codified at 6 U.S.C. § 1133.

[204] Section 1405, Security assessments and plans, codified at 6 U.S.C. § 1134. The statute prohibits requiring security plans under § 1405 from public transportation agencies not receiving grants under § 1406 of the Act, although the exemption may be waived for high-risk agencies with appropriate notification to Congress.

[205] Section 1405(h)(2), codified as 6 U.S.C. § 1134(h)(1).

[206] Section 1406, Public transportation security assistance, codified at 6 U.S.C. § 1135. Subsection (b) provides that allowable uses of funds under this section are as follows:

> (1) Capital uses of funds, including—
>
> (A) tunnel protection systems;
>
> (B) perimeter protection systems, including access control, installation of improved lighting, fencing, and barricades;
>
> (C) redundant critical operations control systems;
>
> (D) chemical, biological, radiological, or explosive detection systems, including the acquisition of canines used for such detection;
>
> (E) surveillance equipment;
>
> (F) communications equipment, including mobile service equipment to provide access to wireless Enhanced 911 (E911) emergency services in an underground fixed guideway system;
>
> (G) emergency response equipment, including personal protective equipment;
>
> (H) fire suppression and decontamination equipment;
>
> (I) global positioning or tracking and recovery equipment, and other automated-vehicle-locator-type system equipment;
>
> (J) evacuation improvements;
>
> (K) purchase and placement of bomb-resistant trash cans throughout public transportation facilities, including subway exits, entrances, and tunnels;
>
> (L) capital costs associated with security awareness, security preparedness, and security response training, including training under section 1408 and exercises under section 1407;
>
> (M) security improvements for public transportation systems, including extensions thereto, in final design or under construction;
>
> (N) security improvements for stations and other public transportation infrastructure, including stations and other public transportation infrastructure owned by State or local governments; and
>
> (O) other capital security improvements determined appropriate by the Secretary.
>
> (2) Operating uses of funds, including—
>
> (A) security training, including training under section 1408 and training developed by institutions of higher education and by nonprofit employee labor organizations, for public transportation employees, including frontline employees;
>
> (B) live or simulated exercises under section 1407;
>
> (C) public awareness campaigns for enhanced public transportation security;
>
> (D) canine patrols for chemical, radiological, biological, or explosives detection;
>
> (E) development of security plans under section 1405;
>
> (F) overtime reimbursement including reimbursement of State, local, and tribal governments, for costs for enhanced security personnel during significant national and international public events;
>
> (G) operational costs, including reimbursement of State, local, and tribal governments for costs for personnel assigned to full-time or part-time security or counterterrorism duties related to public transportation, provided that this expense totals no more than 10 percent of the total grant funds received by a public transportation agency in any 1 year; and
>
> (H) other operational security costs determined appropriate by the Secretary, excluding routine, ongoing personnel costs, other than those set forth in this section.

[207] Section 1408, Public transportation security training program, codified at 6 U.S.C. § 1137.

[208] Section 1414, Security Background Checks of Covered Individuals for Public Transportation, Pub. L. No. 110-53, 121 Stat. 419, codified at 6 U.S.C. § 1143.

[209] 6 U.S.C. § 1143(e); 49 C.F.R. pt. 1570; Department of Homeland Security, Transportation Security Administration, Interim Final Rule, *False Statements Regarding Security Background Check*, Fed. Reg. 73, No. 148, 44665, July 31, 2008, http://edocket.access.gpo.gov/2008/pdf/E8-17515.pdf.

2. Federal Agencies

The DHS, TSA, USDOT, and FTA have issued rulemakings and guidance related to CII and SSI that are applicable, either directly or by analogy, to treatment of security information in competitive bidding. This section discusses these federal activities on an agency-by-agency basis.

DHS/TSA.—DHS has issued several rulemakings related to CII and SSI. The first was the final rule that transferred aviation security authority from FAA to TSA. The second related to the PCII Program. The third related to SSI procedures. Those aspects of the rulemakings most relevant to the arena of competitive bidding are summarized here. Nonregulatory activities that may prove helpful in developing policies for handling security information in the competitive bidding context are also addressed.

Transfer of aviation security authority:[210] Under the rule, the then–Under Secretary (now TSA Administrator) has authority for determining what information is SSI and what persons are required to protect it, while the modal administrators are responsible for protecting the information. The rule expands the persons responsible for protecting SSI beyond the universe covered by 14 C.F.R. § 191.5 because the rule covers each person for which a vulnerability assessment has been "authorized, approved, or funded by DOT, irrespective of mode of transportation."[211]

CII: DHS issued a notice of proposed rulemaking (NPRM) on establishing procedures to implement Section 214 of the HSA in April 2003. DHS issued an interim final rule (IFR) the following year. In the notice promulgating the IFR, DHS stated that in the case of information that qualified as both CII and SSI, federal employees must comply with the more stringent CII requirements. However, the department noted:

> In practice, the situations in which information constitutes both SSI and Protected CII may be limited. For the most part, information that is SSI is created by TSA or is required to be submitted to TSA or to another part of the Federal government. Therefore, it ordinarily will not be voluntarily submitted, which is a required element for Protected CII designation. In addition, SSI might or might not relate to critical infrastructure assets.[212]

In addition, the notice made clear that while the regulation covers information that DHS did not exercise legal authority to obtain even if it was involuntarily submitted to other agencies, submission of such information to DHS does not affect the obligation of such other federal agencies to disclose the information submitted to them.[213] DHS rejected comments requesting that the regulation provide for segregating submitted information so that only information absolutely necessary to protect critical infrastructure is withheld.[214]

The CII regulation was amended in 2006 when DHS issued a final rule amending the 2004 IFR. The final rule's procedures apply to "all Federal, State, local, and tribal government agencies and contractors that have access to, handle, use, or store critical infrastructure information that enjoys protection under the Critical Infrastructure Information Act of 2002."[215] DHS noted that it had added a definition of "in the public domain" to the final rule, drawing in part on the statutory language and adding "information regarding systems, facilities, or operational security, or that is proprietary, business sensitive, or which might be used to identify a submitting person or entity."[216] DHS rejected comments that called for excluding from the definition of "voluntary" information submitted to other federal agencies pursuant to their legal authority.[217] Thus information that otherwise meets the definition of CII, is required to be submitted to another agency, and is voluntarily submitted to DHS must still be treated as CII by DHS and any entity to which DHS discloses the information. However, it appears that if information is submitted to another agency, that agency need not treat the information as confidential, even if the information is identical to information submitted to DHS as CII.[218]

DHS again rejected comments requiring what it terms "portion marking" (segregating CII and non-CII) and extended CII protection to "any information, statements or other material reasonably necessary to explain the CII, put the CII in context, or describe the importance or use of the CII."[219] DHS highlighted criminal and administrative penalties for unauthorized release of information.[220] In addition, DHS eliminated two criteria for allowing a loss of protected status: The fact that the information "is publicly available through legal

---

[210] Department of Transportation, Federal Aviation Administration, Transportation Security Administration, *Civil Aviation Security Rules*, Fed. Reg. 67, No. 36, 8340, Feb. 22, 2002, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2002_register&docid=02-4081-filed.pdf.

[211] *Id*. at 8342.

[212] Department of Homeland Security, Office of the Secretary, Interim Final Rule, 6 C.F.R. pt. 29, *Procedures for Handling Critical Infrastructure Information*, Fed. Reg. 69, No. 34, 8074, 8076, Feb. 20, 2004, http://edocket.access.gpo.gov/2004/pdf/04-3641.pdf.

[213] *Id*.

[214] *Id*. at 8078–79.

[215] Department of Homeland Security, Office of the Secretary, Final Rule, 6 C.F.R. pt. 29, *Procedures for Handling Critical Infrastructure Information*, Fed. Reg. 71, No. 170, 52262, Sept. 1, 2006, http://edocket.access.gpo.gov/2006/pdf/06-7378.pdf. *See* STEVENS & TATELMAN, *supra* note 34, at CRS-18–19.

[216] *Id*. at 52262–63.

[217] *Id*.

[218] Nicholas Bagley, *Benchmarking, Critical Infrastructure Security, and the Regulatory War on Terror*, 43 HARV. J. ON LEGISLATION 47, 68 (2006), at 57 (citing 6 C.F.R. § 29.3(a) (2005)).

[219] Department of Homeland Security, Office of the Secretary, Final Rule, 6 C.F.R. pt. 29, *Procedures for Handling Critical Infrastructure Information*, Fed. Reg. 71, No. 170, 52262, 52264, Sept. 1, 2006, http://edocket.access.gpo.gov/2006/pdf/06-7378.pdf.

[220] *Id*. at 52267.

means" was deleted because this was not a basis under the CIIA. The fact that DHS requires the information was rejected as a basis for allowing a loss of protected status because DHS interprets the definition of voluntary to be retrospective only.[221] Finally, DHS clarified that contractors of state and local governments can receive CII under the same conditions as federal contractors, i.e., engaged in the performance of services in support of the purposes of the CIIA, with strict limitations on further disclosure of the information.[222]

SSI Interim Final Rule:[223] In 2004 DHS issued an IFR on SSI, which promulgated identical regulatory standards for USDOT and TSA under 49 C.F.R. Parts 15 and 1520.[224] The rule was intended to extend the protection of aviation SSI to maritime SSI generated pursuant to the Maritime Transportation Security Act of 2002.[225] The *Federal Register* notice described the rules as requiring employees, contractors, grantees, and agents of both departments to follow the rules' SSI requirements.[226] The notice stated that the rule largely incorporated the substance of the existing regulation, but streamlined and consolidated some provisions and expanded others. For example, the IFR expanded the definition of vulnerability assessment.[227] Under this expanded definition, if a covered person creates a vulnerability assessment at his or her own initiative, but intends to provide the vulnerability assessment to USDOT or DHS in support of a federal security program, the vulnerability assessment is SSI.[228] The interim rule also:

- Introduced the concept of "covered person."[229]
- Designated contract proposals and attendant negotiations for grants and contracts to the extent that the subject matter relates to specific aviation or maritime transportation security measures.[230]
- Clarified that the agency may determine that information is not SSI, even though it might appear to be covered by one of the regulatory categories.
- Is applicable in particular when due to changes in circumstances information is no longer sensitive.[231]
- Added marking requirements for SSI.[232]
- Clarified that if information is both CII and SSI, any covered person who is a federal employee must comply with the more restrictive CII requirements.[233]
- Added provisions describing when federal employees and contractors have need to know SSI.[234]
- Added a provision permitting TSA/Coast Guard to require security background check and imposition of safeguard requirements/procedures before providing SSI.[235]
- Added provisions allowing the department to authorize conditional disclosure of specific records and making clear that such disclosures are not public releases of information for FOIA purposes.[236]
- Added a provision governing required destruction of SSI, which allows state and local government agencies to preserve information required to be preserved under state or local law.[237]

Although the IFR established a broad category of covered persons, TSA noted that persons who fell within the coverage but did not have possession of SSI would not have to meet the disclosure restrictions of 49 C.F.R. § 1520.9.[238] The notice made clear that records that contain SSI and non-SSI may be segregated, with the non-SSI disclosed, provided that the non-SSI is not

---

[221] *Id*. at 52265.

[222] *Id*. at 52268–69.

[223] *See* MITCHEL A. SOLLENBERGER, SENSITIVE SECURITY INFORMATION (SSI) AND TRANSPORTATION SECURITY: BACKGROUND AND CONTROVERSIES, CRS Report to Congress (2004), www.fas.org/sgp/crs/RS21727.pdf.

[224] Department of Transportation, Office of the Secretary, Department of Homeland Security, Transportation Security Administration, Interim Final Rule, *Protection of Sensitive Security Information*, Fed. Reg. 69, No. 96, 28066, May 18, 2004, http://edocket.access.gpo.gov/2004/pdf/04-11142.pdf.

[225] Pub. L. No. 107-295, 116 Stat. 2064, Nov. 25, 2002. *See also* Department of Homeland Security, Coast Guard, Final Rule, *Vessel Security*, Fed. Reg. 68, No. 204, 60483, Oct. 22, 2003; Department of Homeland Security, Coast Guard, Final Rule, *Facility Security*, Fed. Reg. 68, No. 204, 60515, Oct. 22, 2003.

[226] Department of Transportation, Office of the Secretary, Department of Homeland Security, Transportation Security Administration, Interim Final Rule, *Protection of Sensitive Security Information*, Fed. Reg. 69, No. 96, 28066, May 18, 2004, http://edocket.access.gpo.gov/2004/pdf/04-11142.pdf.

[227] *Id*. at 28070, 28079, 28082. Before the interim final rule, vulnerability assessment was defined as "any examination of a transportation system, vehicle, or facility to determine its vulnerability to unlawful interference." As revised under the final rule, the definition became:

> any review, audit, or other examination of the security of a transportation infrastructure asset; airport; maritime facility, port area, vessel, aircraft, train, commercial motor vehicle, or pipeline, or a transportation-related automated system or network, to determine its vulnerability to unlawful interference, whether during the conception, planning, design, construction, operation, or decommissioning phase. A *vulnerability assessment* may include proposed, recommended, or directed actions or countermeasures to address security concerns.

49 C.F.R. §§ 15.3, 1520.3.

[228] Department of Transportation, Office of the Secretary, Department of Homeland Security, Transportation Security Administration, Interim Final Rule, *Protection of Sensitive Security Information*, Fed. Reg. 69, No. 96, 28066, 28071, May 18, 2004, http://edocket.access.gpo.gov/2004/pdf/04-11142.pdf.

[229] *Id*.

[230] *Id*. at 28072.

[231] *Id*.

[232] *Id*. at 28074.

[233] *Id*.

[234] *Id*.

[235] *Id*.

[236] *Id*. at 28075.

[237] *Id*.

[238] *Id*. at 28074.

otherwise properly exempt from disclosure.[239] This assertion is somewhat undercut by the statement "if it is impractical to redact the requested information from the record, the entire record is withheld."[240] The IFR did not address the issue of establishing that specific material constitutes SSI, as the rule deems categories of information to be SSI.

A number of parties filed comments in response to the request for comments to the IFR. Although TSA did not respond to the comments, some of the comments illuminate issues of interest in handling SSI in competitive bidding situations.

Some commenters urged expanded coverage. For example, the Port Authority of New York and New Jersey[241] asked that the definition of covered person be expanded to facilitate information sharing with other governmental entities and that modes such as rail and bus transportation be explicitly covered as well. The Massachusetts Port Authority (Massport)[242] specifically requested that the regulations provide authority similar to that in Section 15.11(b)(2) for public agencies to share SSI with bidders and contractors, rather than requiring the agencies to rely on subparagraphs 15.11(a)(1) and (a)(4). Massport also recommended expanding specifications under Section 15.5(b)(4).

The Coalition of Journalists for Open Government (CJOG)[243] commented that the rule would result in too much information being designated SSI. CJOG specifically raised the concern that local and state officials may be required to deny access to records that would otherwise be available under state and local open records requirements. Other CJOG points relevant to procurement include the following recommendations:

- The regulation require that limited numbers of trained individuals be assigned to designate SSI.
- The regulation provide criteria for SSI designation.
- Lists of infrastructure assets submitted by state and local government agencies not be automatically deemed SSI without some evaluation of whether the assets have some relation to security.
- Records that deal with contracts, public funding, and operational issues that implicate accountability issues be subject to special review.
- The regulation adopt the Department of Justice's (DOJ) standard of withholding nonexempt information along with exempt information only if the two are "inextricably intertwined."

CJOG cautioned that allowing the government to designate "other information" as SSI was an invitation to abuse, particularly given the potentially large number of people allowed to designate SSI. The comment also expressed concern that the requirements for marking SSI did not call for segregating non-SSI, thereby effectively sealing off entire documents regardless of security implications.

The Silha Center for the Study of Media Ethics and Law also commented on the dangers of over-designating information as SSI. Specifically the center argued that the IFR should be modified to more narrowly define SSI, reduce the scope of "covered persons" to those actually having access to SSI, and to require the review of SSI after a set time, potentially declassifying rather than destroying it. Moreover, the center took the position that to prevent over-withholding of information, information should be reviewed to determine whether its disclosure presents an actual danger to transportation security, rather than automatically conferring SSI designation on classes of information. In addition, the center argued against labeling an entire record SSI when only a portion of the record actually contains SSI. In particular, the center argued against allowing the IFR to trump state disclosure laws by requiring the withholding of information the release of which has not been shown to cause substantial harm to transportation safety.[244]

In 2005 DHS issued a correction to the IFR, eliminating "aviation or maritime" from 49 C.F.R. § 15.11 and 49 C.F.R. § 1520.11 to make clear that regardless of mode, vulnerability assessments and other documents properly designated as SSI may be shared with covered persons who meet the need to know requirements.[245]

Rail Security Rule:[246] In December 2006, TSA issued an NPRM for Rail Transportation Security.[247] Much of the notice related to security inspections, but the notice also proposed clarifications to SSI requirements. TSA noted that the proposed rule was consistent with the Memorandum of Understanding executed between DHS and USDOT[248] to ensure collaboration as required under Homeland Security Presidential Directive 7.[249] The no-

[239] *Id*. at 28075.

[240] *Id*. at 28074.

[241] TSA-2003-15569-0011. Accessible from www.regulations.gov/search/Regs/home.html#docketDetail?R=TSA-2003-15569.

[242] *Id*. at 15569-0020.

[243] *Id*. at 15569-0010.

[244] Comments of the Silha Center for the Study of Media Ethics and Law on Interim Final Rule, *Protection of Sensitive Security Information*, July 16, 2004, TSA-2003-15569-0013, www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480313ddb (accessed Sept. 10, 2009).

[245] Protection of Sensitive Security Information; Technical Amendment, 70 Fed. Reg. 1379 (Jan. 7, 2005), http://edocket.access.gpo.gov/2005/pdf/05-366.pdf.

[246] 49 C.F.R. pts. 1520 and 1580.

[247] Department of Homeland Security, Transportation Security Administration, Proposed Rule, *Rail Transportation Security*, Fed. Reg. 71, No. 245, 76852, Dec. 21, 2006, http://edocket.access.gpo.gov/2006/pdf/E6-21512.pdf.

[248] Memorandum of Understanding Between the Department of Homeland Security and the Department of Transportation on Roles and Responsibilities, Sept. 2004. Accessed Sept. 13, 2009, at www.dot.gov/ost/ogc/DHS-DOT.PDF.

[249] Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection (HSPD–7), Dec. 17, 2003,

tice made clear TSA's position that although 49 C.F.R. Part 1520 primarily relates to aviation and maritime security information, vulnerability assessments and threat assessments for all modes of transportation are considered SSI.[250] TSA proposed to extend the definition of covered persons to include rail transit systems, explicitly requiring them to restrict "distribution, disclosure, and availability of SSI to persons with a need to know, and refer all requests for SSI by other persons to TSA or the applicable component or agency within DOT or DHS." [251] In addition, TSA proposed to clarify that "any review, audit, or other examination of the security" of a rail transit system or facility "that is directed, created, held, funded, or approved by DOT or DHS, or that will be provided to DOT or DHS in support of a Federal security program, is SSI." TSA also proposed to extend coverage to specific details of rail transportation security measures, security training materials for those carrying out rail transportation security measures required or recommended by DHS or USDOT, and lists identifying critical rail infrastructure assets. TSA also sought comment on whether it should protect as SSI "any other information that may be created under this rule."[252] TSA noted that the training materials contain descriptions of security measures that could be used by terrorists to defeat security procedures. In addition, while TSA proposed to expand the lists of critical infrastructure assets to include rail transportation, the information would only be covered if it is prepared by DHS or USDOT or prepared by a state or local government agency and submitted to DHS or USDOT.[253]

While most of the transit comments related to concerns about unannounced inspections and other operational requirements, a number of the comments related to SSI. The Oregon DOT commented that the expansion of the "need to know" requirement raises issues concerning the need for states to access information now required under partnership programs with the Federal Railroad Administration and FTA.[254] Chicago also suggested that the rule should specify that state and local governments have access to SSI.[255] New Jersey asked that rail security information be accorded "enhanced" protection status.[256] The City of Cleveland suggested that the rule require employees of covered entities to undergo background investigations, using a federally-established list of disqualifying crimes in hiring.[257] The Texas[258] and Florida[259] DOTs also raised concerns that the proposed requirements for SSI would inhibit exchange of information with state oversight agencies.

On the other hand, CJOG raised concerns that the rule would result in a vast range of information about rail and transit management and operations being shielded from public view, eliminating public oversight. In particular, CJOG questioned the fact that the proposed rule would allow the operators to determine what information is included in vulnerability assessments and automatically treated as SSI, potentially resulting in the withholding of information traditionally disclosed at the state and local level. CJOG suggested that TSA narrow the definition of SSI and review filings and identify information that does not warrant protection. Finally, CJOG advocated for sunsetting the SSI designation, subject to potentially extending the protection for specific information for which, based on subsequent review, further withholding was deemed necessary.[260]

In November of 2008, TSA issued the final rule.[261] TSA made two changes to the NPRM provisions on SSI.[262] First, TSA added rail to the categories of research and development information protected under 49 C.F.R. § 1520.5(b)(15). Second, TSA added state, local,

www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1. HSPD–7 required the Secretary of DHS to coordinate protection activities for specified critical infrastructure sectors, including mass transit.

[250] Department of Homeland Security, Transportation Security Administration, Proposed Rule, *Rail Transportation Security*, Fed. Reg. 71, No. 245, 76852, 76862, Dec. 21, 2006, http://edocket.access.gpo.gov/2006/pdf/E6-21512.pdf.

[251] *Id*.

[252] *Id*.

[253] *Id*. at 76867.

[254] Oregon Department of Transportation, Kelly Taylor, Rail Division Administrator, Feb. 20, 2007, at 3, TSA-2006-26514-0095, www.regulations.gov/search/Regs/home.html#documentDetail?R=09000064802aa82c.

[255] Chicago Department of Transportation, Cheri Heramb, Acting Commissioner, Jan. 15, 2007, TSA-2006-26514-0038, www.regulations.gov/search/Regs/home.html#documentDetail?R=09000064802aa7e6.

[256] New Jersey Office of Homeland Security & Preparedness, Richard L. Canas, Director, Feb. 20, 2007, at 2, TSA-2006-26514-0072, www.regulations.gov/search/Regs/home.html#documentDetail?R=09000064802aa810.

[257] Shirley A. Tomasello, Assistant Law Director, Department of Law, City of Cleveland, Feb. 16, 2007, at 7, TSA-2006-26514-0067, www.regulations.gov/search/Regs/home.html#documentDetail?R=09000064802aa80a.

[258] Texas Department of Transportation, Michael W. Behrens, P.E., Executive Director, Feb. 20, 2007, TSA-2006-26514-0078, www.regulations.gov/search/Regs/home.html#documentDetail?R=09000064802aa815.

[259] Florida Department of Transportation, Mike Johnson, Administrator, Transit Operations, Feb. 1, 2007, TSA-2006-26514-0012, www.regulations.gov/search/Regs/home.html#documentDetail?R=09000064802aa7c5.

[260] Coalition of Journalists for Open Government, Pete Weitzel, Feb. 20, 2007, TSA-2006-26514-0053, www.regulations.gov/search/Regs/home.html#documentDetail?R=09000064802aa7fb.

[261] Department of Homeland Security, Transportation Security Administration, Final Rule, *Rail Transportation Security*, Fed. Reg. 73, No. 229, 72130, Nov. 26, 2008, http://edocket.access.gpo.gov/2008/pdf/E8-27287.pdf.

[262] *Id*. at 72134.

and tribal government employees, contractors, and grantees to the list under 49 C.F.R. § 1520.11(b) of persons with a potential need to know SSI. In its response to comments, TSA reiterated: "TSA does not intend to protect information as SSI that would not be detrimental to transportation security if publicly disclosed."[263]

Directives: TSA has issued a number of directives that provide guidance on managing SSI. These directives are not publicly available,[264] and so are not summarized here. Transit agencies should be able to obtain them directly from TSA.

Guidance: DHS has issued guidance for public transportation agencies on conducting background checks.[265] DHS suggests that transit agencies may use criminal background checks for employees and contract workers with unmonitored access to designated critical infrastructure. DHS suggests that in structuring those requirements, the agencies look to the federal security requirements for hazardous material drivers and port transportation workers.[266] DHS also suggests that transit agencies consider using the Social Security Number Verification System and the Systematic Alien Verification for Entitlements database to determine a noncitizen's immigration status, as well as periodically reinvestigating employees and contractors, "particularly those with access to sensitive information or security critical facilities."[267]

Nonregulatory activity: DHS/TSA nonregulatory activity may provide models for transit authorities in controlling access to security information. Two activities may be of particular interest. First, DHS requires its employees and contractors to sign nondisclosure agreements (NDAs), prohibiting them from disclosing a wide range of sensitive but unclassified information to the public.[268] The scope of those NDAs was challenged.[269] Second, TSA has implemented a process for conducting SSI Access Threat Assessments.[270] These threat assessments are conducted on any persons seeking access to SSI for use in a civil proceeding under Section 525(d) of the Department of Homeland Security Appropriations Act of 2007, *supra*. The assessments include a fingerprint-based Criminal History Records Check and a name-based check against terrorism and other databases to determine "whether the individual poses or is suspected of posing a threat to transportation or national security."[271] TSA provides a Privacy Act notice to each party seeking access to SSI for civil court proceedings to obtain informed consent before TSA conducts the threat assessment. TSA notifies covered individuals if the agency determines, based on the threat assessment, that the individuals are not eligible to access particular SSI. The individuals may then appeal the decision, including making requests to correct errors in the individuals' records.

USDOT—USDOT has issued several rulemakings related to SSI. The first was the final rule that transferred aviation security authority from FAA to TSA. The second was the series of rulemaking related to SSI procedures.

Transfer of aviation security authority: See discussion under DHS/TSA, *supra*.

Protection of SSI regulation: The USDOT regulation, issued jointly with the TSA regulation, was virtually identical to the TSA regulation. See discussion under DHS/TSA, *supra*.

FTA—Regulations, circulations, and guidance issued by FTA cover documentation related to various transit security plans and designs. Such documentation clearly raises FOIA/SSI issues; to the extent that contractors are involved in either preparing or executing the plans and designs, procurement security is also implicated. This section discusses guidance related, directly or indirectly, to SSI and other security documentation; security-related circulars and regulations for major capital investments and fixed rail; grant requirements and recommendations related to security procurements; and third party contracting security requirements.

General Document Control Guidance: Following the events of 9/11, FTA issued general guidance concerning document control measures that transit agencies should undertake for security critical systems and facilities. These measures included maintaining an appropriate level of security around plans and designs of operating and maintenance facilities and infrastructure (e.g., tunnels, bridges, electrical substations), and maintain-

[263] *Id*. at 72147.

[264] 49 C.F.R. Part 659 Reference Guide, June 22, 2005, at 27, http://transit-safety.volpe.dot.gov/publications/sso/49CFRPart659_FinalRule/49CFR659_Reference_Guide.pdf (accessed Sept. 15, 2009).

[265] Additional Guidance on Background Checks, Redress and Immigration Status, www.tsa.dhs.gov/assets/pdf/guidance_employee_background_checks.pdf.

[266] Disqualifying crimes applicable to hazardous material drivers and transportation workers at ports: 49 C.F.R. § 1572.103; appeal and waiver process: 49 C.F.R. pt. 1515.

[267] Additional Guidance on Background Checks, Redress and Immigration Status, www.tsa.dhs.gov/assets/pdf/guidance_employee_background_checks.pdf.

[268] PATRICE MCDERMOTT, WHO NEEDS TO KNOW?: THE STATE OF PUBLIC ACCESS TO FEDERAL GOVERNMENT INFORMATION 135 (2007); Spencer S. Hsu, *Homeland Security Employees Required to Sign Secrecy Pledge*, WASH. POST, Nov. 16, 2004, at A23, www.washingtonpost.com/wp-dyn/articles/A52977-2004Nov15.html (accessed Mar. 4, 2009); Department of Homeland Security Non-Disclosure Agreement, www.tsa.gov/assets/pdf/NDA_v2.pdf. *See* App. F, *infra*.

[269] *Unions Challenge Department of Homeland Security Non-Disclosure Agreement*, CANADIAN DIMENSION 39.1 (Jan.–Feb. 2005), at 8(2); Hsu, *supra* note 268.

[270] Dep't of Homeland Security, Privacy Impact Assessment for Threat Assessments for Access to Sensitive Security Information for Use in Litigation, Dec. 28, 2006, www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_ssi.pdf (accessed Sept. 23, 2009).

[271] *Id.* at 4.

ing an appropriate level of security around documentation for security detection systems.[272]

Designation, Marking, and Control of SSI:[273] FTA's SSI guidance was issued with the express purpose of helping transit agencies to prevent "the unauthorized disclosure or dissemination of SSI while preserving the public's 'right to know' about transit systems and operations."[274] Under this guidance document, FTA defines transit SSI as "any information or record whose disclosure may compromise the security of the traveling public, transit employees, or transit infrastructure," including "data, documents, engineering drawings and specifications, and other records whose disclosure could increase the agency's risk of harm."[275] The types of records that apply to transit agencies are identified:[276]

- Security programs and contingency plans issued, established, required, received, or approved by USDOT or DHS.
- Vulnerability assessments that are directed, created, held, funded, or approved by USDOT or DHS, or that will be provided to either agency in support of a federal security program.
- Threat information held by the federal government concerning transportation, transportation systems, and cyber infrastructure, including sources and methods used to gather or develop the information.

Both the TSA Administrator and the Secretary of USDOT may determine that additional information constitutes SSI.

In addition to appropriately handling the SSI listed above, the transit agency is advised to review the following records for SSI:[277]

- Security program plans and procedures that include vulnerability records or specific tactics for security operations.
- Security contingency plans and records.
- Records that reveal system or facility vulnerabilities (e.g., maps, detailed facility drawings, detailed action items from drills and exercises).

According to the guidance, if a portion of a document is SSI, the entire document must be controlled as SSI, and can only be released if the SSI is redacted.[278] If the SSI is placed in an appendix that can be separated from the rest of the document, the remainder of the document can be more widely distributed once the appendix is redacted.[279] This approach clearly applies to contract documents.

The guidance suggests a two-step process under which employees who may generate SSI are knowledgeable enough to recognize potential SSI and to refer it to the employee or committee designated to make SSI determinations for the agency. Making the determination that information could be SSI requires consideration of the agency's threat environment, the public's need to know the information, the availability of similar information from other sources, and the utility of the information to someone intent on causing harm.[280] For example, procurement personnel should be sufficiently knowledgeable about SSI requirements to understand when to refer material to the SSI employee/committee and how to structure contract documents that relate to SSI. The FTA's examples of SSI and non-SSI are included as Appendix F, *infra*.

Any information that is determined to be SSI must be marked to warn that the information is controlled and may only be distributed to persons with a need to know. The guidance provides the mandatory advisory marking, included the required language to use.[281] Only a covered person with a need to know may access SSI. "Need to know" includes requiring the SSI to perform official duties pursuant to a contract or grant. "Covered person" includes the following four categories applicable to transit agencies:[282]

- Persons who have access to SSI.
- Persons employed by, contracted to, or acting for a covered person, including a grantee of DHS or USDOT, and persons formerly in such a position.
- Persons for whom a vulnerability assessment has been directed, created, held, funded, or approved by the USDOT or DHS, or who have prepared a vulnerability assessment that will be provided to either agency in support of a federal security program.
- Persons receiving SSI.

FTA advises that transit agencies establish rules for disseminating SSI to contractors and suggests controlling access by using prequalification, including nondisclosure forms; maintaining secure locations for review of SSI; and covering SSI handling in contracts, including "use, storage, reproduction, dissemination, and return, both on and off of transit property."[283]

---

[272] TSA/FTA Security and Emergency Action Items for Transit Agencies, Document Control, Items 15 and 16, http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/ActionItems/actionlist.asp#Document_Control; FED. TRANSIT ADMIN., U.S. DEP'T OF TRANSP., FY 2009 TRIENNIAL REVIEW WORKSHOPS WORKBOOK 19–13, www.fta.dot.gov/documents/FY2009_TriennialReview_Workbook.pdf; TRANSTECH MANAGEMENT, INC., *supra* note 1, at chs. 2, 3, and Appendices.

[273] CHANDLER, SUTHERLAND, & ELDREDGE, *supra* note 164, at 3.

[274] *Id*. at 1.

[275] *Id*. at 3.

[276] *Id.* at 5.

[277] *Id.*

[278] *Id.* at 8.

[279] *Id.* at 5.

[280] *Id.* at 7–8.

[281] *Id.* at 10.

[282] *Id.* at 11–12.

[283] *Id.* at 13.

The following points concerning SSI control[284] will apply to bid/contract SSI:

- SSI must be stored securely. If possible, the SSI should be stored by the owner or originator.
- When SSI is in use, the custodian, if required to suspend work temporarily, must secure the records.
- Reproduction must be kept to the minimum required for agency business, with copies protected as the originals.
- Transmission must protect against unauthorized disclosure.
- Return of SSI must be assured.
- Destruction must be by a method that precludes recognition or reconstruction.
- Employees and contractors likely to handle SSI should be trained on handling requirements.

FTA Circular 5800.1: Under 49 U.S.C. § 5327(a), applicants and recipients of major capital project funding must address safety and security management as part of their project management plan. FTA has implemented this statutory mandate by issuing guidance that calls on recipients to prepare a Safety and Security Management Plan (SSMP) as part of the project management plan required by 49 U.S.C. § 5327(a).[285] Chapter II of FTA Circular 5800.1 includes the following provisions:

- Establishing a program that identifies and assesses security vulnerabilities throughout the project development process.
- Establishing a process for documenting and tracking actions taken to address the vulnerability assessment.
- Establishing security requirements for the project, based on applicable safety and security codes, guidelines, and standards established by government agencies and industry associations.
- Developing documentation to convey security rules and procedures for the project to employees, contractors, and oversight agencies. Documents may include security plans, as well as operating and maintenance procedures and manuals.
- Establishing qualifications and training programs for operating and maintenance personnel, which programs must address security elements.
- Identifying any security analyses contractors must perform for the construction site.

Section 2, Chapter IV, of the circular provides that the SSMP include procedures for managing SSI. Contracting out any of the activities provided for under Chapter II or the development of procedures required under Chapter IV could have ramifications for procurement security.

Chapter II of Circular 5800.1 expressly addresses protection of SSI. Recipients with major capital projects covered by 49 C.F.R. Part 633 are directed to document or reference their procedures for managing SSI in the SSMP, which procedures are expected to extend to their project contractors. In addition, any SSI submitted to FTA and project management oversight contractors during the project management oversight process will be exempt from disclosure under FOIA.[286] Finally the circular directs the recipient to have SSI handling procedures.[287]

Although SSMPs are required by law only for major capital investment projects, FTA encourages all transit systems to develop transit system security program plans. Such plans are also considered SSI. FTA's Triennial Review contractors may only examine them on site at the time of the Triennial Review.[288]

State Safety Oversight of Rail Fixed Guideway Systems: [289] The regulation requires transit agencies to develop system security plans for rail fixed guideway systems and state oversight agencies to review those plans. The plans must contain five elements,[290] which may include SSI:

- Identification of policies, goals, and objectives for the security program.
- Documentation of the rail transit agency's threat and vulnerability process.
- Identification of controls in place that address the personal security of passengers and employees.
- Documentation of the agency's process for conducting internal security reviews to evaluate compliance and measure effectiveness of the system security plan.
- Documentation of the agency's process for making its system security plan and accompanying procedures available to the oversight agency for review and approval.

[284] *Id.* at 15–17.

[285] Safety and Security Management for Major Capital Projects: Notice of Final Circular, 72 Fed. Reg. 34339 (June 21, 2007), http://edocket.access.gpo.gov/2007/pdf/E7-11970.pdf; FTA Circular 5800.1, Safety and Security Management Guidance for Major Capital Projects (Aug. 1, 2007), www.transportation.org/sites/scopt/docs/FTA%20C%205800%201%20-%20FINAL%20Safety%20and%20Security%20Management%20Plan-1.pdf. *See also* Frequently Asked Questions, http://transit-safety.volpe.dot.gov/publications/security/Safety%20%20Security%20frequent%20questions.pdf.

[286] FTA Circular 5800.1, II.4, at II-5.

[287] FTA Circular 5800.1, IV.2.b., at IV-2. *See also* FED. TRANSIT ADMIN., *supra* note 272, at 19-7, noting requirement to review security and emergency management plans.

[288] FED. TRANSIT ADMIN., *supra* note 272, at 19-7.

[289] 49 U.S.C. § 5330; 49 C.F.R. pt. 659, Rail fixed guideway systems; State safety oversight, www.access.gpo.gov/nara/cfr/waisidx_08/49cfr659_08.html; 49 C.F.R. Part 659 Reference Guide, http://transit-safety.volpe.dot.gov/publications/sso/49CFRPart659_FinalRule/49CFR659_Reference_Guide.asp.

[290] 49 C.F.R § 659.23, *System security plan: contents*.

The requirements governing state oversight of the security of rail fixed guideway systems through designated oversight agencies do raise confidentiality issues concerning the state agency's handling of security plans, for example if such plans are considered public records under state public records law. The regulation does not require public availability of the system security plan;[291] does require the oversight agency to explain how it will protect the system security plan from public disclosure; [292] and authorizes the oversight agency to prohibit a transit agency from publicly disclosing the system security plan.[293] FTA recommends that the oversight agency only take possession of a system security plan if the agency can maintain the plan's confidentiality under state sunshine laws.[294] As FTA notes in its Part 659 guidance, the review of system security plans must comply with 49 C.F.R. Part 1520.[295] According to FTA guidance, the process required under Section 659.23(e) must be documented "according to procedures established to prevent public disclosure of these materials."[296] These oversight requirements also raise procurement concerns if a state contracts out its oversight responsibilities or if a transit agency contracts out the development[297] or review[298] of its systems security plan.

Procurement of Security-Related Goods and Services: There are a number of grant requirements and FTA recommendations that result in transit agencies procuring security-related goods and services and having to manage information related to those procurements. For example, recipients of Urbanized Area Formula Grants must certify annually that they are spending 1 percent of Urbanized Area Formula Grant Program funds on security projects or that those projects are not necessary.[299] Eligible projects under 49 U.S.C. § 5307 include increased lighting, increased camera surveillance, providing emergency telephone lines, and "any other project intended to increase the security and safety of an existing or planned public transportation system."[300] FTA guidance provides the following more specific examples of appropriate security expenditures: "facility perimeter security and access control systems (e.g., fencing, lighting, gates, card reader systems, etc.), closed circuit television camera systems (at stations, platforms, bus stops and on-board vehicles), security and emergency management planning, training and drills."[301] Agencies may also expend funds to purchase explosive detection equipment. For example, the New York Police Department, which conducts random passenger searches on the New York City subway system, has purchased hand-held devices that can be used "to detect and identify explosives, chemical warfare agents, and toxic industrial chemicals."[302]

Third Party Contracting Security Requirements: Grant recipients are generally responsible for extending federal requirements to third party contractors. [303] While this alone might be sufficient to require grant recipients to require SSI protection from their contractors, SSI requirements are specifically referenced in FTA's third party contracting circular: third party contractors must protect SSI to ensure compliance with the DHS/USDOT statutes and implementing regulations discussed earlier. This requirement includes taking measures to ensure that subcontractors at each tier protect SSI in accordance with applicable law and regulation.[304]

Both the common grant rule and FTA's authorizing legislation[305] require third party procurement procedures that require full and open competition. This requirement covers prequalification,[306] a method that may

[291] 49 U.S.C. § 659.11, *Confidentiality of investigation reports and security plans.*

[292] 49 C.F.R. § 659.15(b)(9).

[293] 49 C.F.R. § 659.21(b).

[294] 49 C.F.R. Part 659 Reference Guide, June 22, 2005, at 13, http://transit-safety.volpe.dot.gov/publications/sso/49CFRPart659_FinalRule/49CFR659_Reference_Guide.pdf (accessed Sept. 15, 2009).

[295] 49 C.F.R. Part 659 Reference Guide, June 22, 2005, at 26–27, http://transit-safety.volpe.dot.gov/publications/sso/49CFRPart659_FinalRule/49CFR659_Reference_Guide.pdf (accessed Sept. 15, 2009). Compliance with 49 C.F.R. pts. 15 and 1520, to the extent applicable, are grants requirements. FTA Master Agreement MA(16), 10-1-2009, at 59, Section 37: Protection of Sensitive Security Information, www.fta.dot.gov/documents/16-Master.pdf .

[296] 49 C.F.R. Part 659 Reference Guide, June 22, 2005, at 28, http://transit-safety.volpe.dot.gov/publications/sso/49CFRPart659_FinalRule/49CFR659_Reference_Guide.pdf (accessed Sept. 15, 2009).

[297] 49 C.F.R. §§ 659.21 System security plan: general requirements, 659.23 System security plan: contents.

[298] 49 C.F.R. § 659.25(b)(9).

[299] FTA Master Agreement MA(16), Oct. 1, 2009, at 61, § 39: Special Provisions for the Urbanized Area Formula Program, e. Public Transportation Security, http://www.fta.dot.gov/documents/16-Master.pdf.

[300] 49 U.S.C. § 5307(d)(1)(J).

[301] FED. TRANSIT ADMIN., *supra* note 272, at 19-4.

[302] *New York City Police Deploy Trace Detectors From Smiths Detection*, THE POLICE CHIEF, vol. 73, no. 9, Sept. 2006, http://policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=1005&issue_id=92006 (Sept. 23, 2009).

[303] FTA Master Agreement MA(16), Oct. 1, 2009, at 15, § 2: Project Implementation, e. Recipient's Responsibility to Extend Federal Requirements to Other Entities, http://www.fta.dot.gov/documents/16-Master.pdf.

[304] FTA Circular 4220.1F, ch. IV, The Recipient's Property and Services Needs and Federal Requirements Affecting Those Needs § 2.a(7), at IV-7; Third Party Contracting Guidance: Notice of Final Circular, 73 Fed. Reg. 56896, 56906 (Sept. 30, 2008), http://edocket.access.gpo.gov/2008/pdf/E8-22914.pdf.

[305] 49 U.S.C. § 5325(a).

[306] FTA Circular 4220.1F, ch. VI, Procedural Guidance for Open Market Procurements, § 1.(c), at VI-2. For a discussion of prequalification procedures in general, *see* Daniel D. McMillan

be used to control contractor access to security information. However, FTA authorizes noncompetitive proposals when disclosure of recipient's needs would compromise national security.[307]

C. Procurement and Contract Management Issues

Maintenance of transit agency records will be subject to USDOT and FTA requirements. These requirements constitute the minimum period that records must be retained; if state law requires longer periods of retention, the stricter requirement will govern. As discussed below, certain FTA guidance on what information to include in procurement records may have implications for how those records must be managed. In addition to USDOT requirements, financial records may be subject to Internal Revenue Code requirements.[308]

USDOT's common grant rule[309] contains requirements for records retention for grantees.[310] While this provision does not apply to contractors, the rule requires grantees to place a similar provision in third party contracts, with the 3-year retention period beginning after all issues are resolved, not when the project is completed.[311]

The FTA Master Agreement requires grantees to maintain "intact and readily accessible" all third party contracts related to a federally funded project for 3 years after the transmission of the final expenditure report.[312] Pursuant to 49 C.F.R. § 18.42, if an action such as litigation or audit involving the records begins before the 3-year retention period expires, the records at issue must be kept until the later of completion of the action and resolution of all issues or the expiration of the otherwise required 3-year period.

Chapter III of FTA's Third Party Contracting Guidance addresses the recipient's responsibilities.[313] Section 3 covers third party contracting capacity, including the need for contract administration, written procurement procedures (subsection a), and record keeping requirements, including procurement history (subsection d). These requirements do not impose lengthier record retention periods than the common grant rule. Section 4 covers audits, suggesting but not mandating that grantees perform audits of third party contracts as part of the contract administration process.

Section 10.3 of FTA's *Best Practices Procurement Manual* summarizes FTA's record retention requirements and provides suggested language for using in third party contracts.[314] Other provisions of the manual that relate to record retention and contents of contract documentation include recommendations to maintain file documentation that includes the statement of work/scope of services;[315] include in the file that documents the selection decision for negotiated procurements a technical evaluation indicating the relative strengths and weaknesses of the proposals, together with the technical risks of any of the approaches considered;[316] and include approvals and disapprovals of contract submittals required by the contract and requests for waivers or deviations from contractual requirements in the contract administration file.[317] Including security information, particularly SSI, in such documentation will affect not only how the transit agency should respond to open records requests, but also how the documentation must be marked and stored.

III. STATE LAW SUMMARY[318]

All 50 states and the District of Columbia have laws requiring public access to government documents,[319]

& Erich R. Luschei, *Prequalification of Contractors by State and Local Agencies: Legal Standards and Procedural Traps*, 27 THE CONSTRUCTION LAWYER 21, Spring 2007, www.jonesday.com/files/Publication/1ccdcb41-cf82-4158-984b-4e97deed5301/Presentation/PublicationAttachment/d36a1308-33b4-4da2-920b-06bde881d321/McMillan_Luschei_2007.pdf (accessed Sept. 25, 2009). N.B.: This article does not address security issues.

[307] FTA Circular 4220.1F, ch. VI, Procedural Guidance for Open Market Procurements, § 3.i(1)(e)2.f, at VI-18.

[308] *See* FTA Frequently Asked Questions: Third Party Procurement—Record Retention, www.fta.dot.gov/funding/thirdpartyprocurement/faq/grants_financing_6218.html.

[309] 49 C.F.R. pt. 18, Uniform administrative requirements for grants and cooperative agreements to State and local governments.

[310] 49 C.F.R. § 18.42.

[311] 49 C.F.R. § 18.36(i)(10) and (11).

[312] Section 8, Reporting, Record Retention, and Access, FTA Master Agreement MA(16), Oct. 1, 2009, at 24, http://www.fta.dot.gov/documents/16-Master.pdf.

[313] FTA Circular 4220.1F, Nov. 1, 2008. This document replaced FTA Circular 4220.1E, the document referenced throughout the BPPM, www.fta.dot.gov/documents/BPPM_fulltext.pdf.

[314] Section 10.3 and other sections of the BPPM cite § 7.i., FTA Circular 4220.1E, as the requirement for record retention. This provision is now covered in FTA Circular 4220.1F, ch. III, The Recipient's Responsibilities, § 3 d.

[315] BPPM 2.4.1 File Documentation, ch. 2, at 17–19.

[316] BPPM 5.4 Documentation of Procurement Actions, ch. 5, at 25–30.

[317] BPPM 9.1 Documentation of Contract Administration, ch. 9, at 1–12.

[318] State public records requirements may apply to all governments within the state. *See*, *e.g.*, Public Records Act for Washington Cities and Counties, Report Number 61, May 2007, Municipal Research and Services Center, www.mrsc.org/Publications/pra06.pdf (accessed Apr. 1, 2009). In addition, local governments may have their own record retention and disclosure requirements.

[319] Michael W. Field, *Rhode Island's Access to Public Records Act: An Application Gone Awry*, 8 ROGER WILLIAMS U. L. REV. 293 (2003), at 294; Leanne Holcomb & James Isaac, *Wisconsin's Public-Records Law: Preserving the Presumption of Complete Public Access in the Age of Electronic Records*, 2008 WIS. L. REV. 515, 517 (2008). The Reporters Committee for Freedom of the Press maintains an online Open Government Guide analyzing all 50 state statutes, www.rcfp.org/ogg/index.php?AL22 (accessed July 28, 2009).

although, as discussed below, the scope of those laws differs. State requirements for disclosing or withholding information, as well as for maintaining records, are clearly relevant to information that is not created pursuant to federal mandates or shared with federal agencies. Even where security information is submitted for purposes of completing federal grants or otherwise complying with federal law, state law may be relevant. For example, DHS recommends that applicants consult state and local laws concerning the release of information in considering what information to report in grant applications, needs assessments, and strategic planning.[320] Moreover, as discussed below, state procedural requirements must be considered even if information requested is clearly exempt from disclosure under federal law.

A myriad of state laws may affect a transit agency's need to disclose or withhold information contained in contract documents, as well as to maintain contract records. Relevant types of state statutes typically include public records/freedom of information, records management, and public contract laws. States may have transportation law titles that contain relevant provisions, as well as homeland security requirements that are relevant. Other categories of state laws that may have requirements for maintaining confidentiality of security information include state building codes (requirements for safe storage and secure handling of engineering and construction plans for critical structural components)[321] and emergency preparedness/disaster response laws (disaster preparedness laws).[322]

Public records laws are likely to be the most important sources of disclosure requirements, while records management laws are most likely to be the source of requirements concerning what records a transit agency must maintain and for how long. The actual definition of "public records" under state law may reside in either type of statute. Public contract laws may have requirements for both disclosure and record retention.

Balancing of public interests is a principle that public agencies often apply in the open records arena, sometimes resulting in disclosure being found to be in the public interest and sometimes not.[323] Depending on state law, public agencies, including transit agencies, may be called upon to explicitly balance competitive procurement and security considerations. These considerations may appear to be in conflict on their face. For example, the Northern Palm Beach County Improvement District questioned its authority to release building plans to contractors for purposes of meeting its obligations under Florida's competitive bidding requirements, in light of Section 199.07(3)(ee), Florida Statutes, which exempts certain public building plans from the mandatory disclosure requirements under Florida's constitution. In response, the Florida Attorney General advised that the competitive bidding and security provisions should be read together "in a fashion that will allow them to operate together and give the fullest effect to each." Accordingly, the Attorney General advised that the Improvement District should release the building designs to contractors as necessary to comply with competitive bidding requirements, but should require that the recipients maintain the exempt status of the information.[324]

In addition to coming under public records statutes, requests for security information may arise in litigation. In such cases the agency may reasonably request that the recipient execute an NDA.[325]

A. Public Records Laws[326]—Disclosure Requirements

A number of issues related to public records disclosure requirements are relevant to understanding how those requirements affect managing security information in the competitive procurement process. These include the applicability of state public records laws to public transit agencies in the state, the definition of public record under state law, whether state law includes a presumption of disclosure or of denial, the approach to exemptions under state law, the burden of proof on classifying information as exempt from disclo-

[320] Fiscal Year 2007 Homeland Security Grant Program, Urban Areas Security Initiative: Nonprofit Security Grant Program, Program Guidance and Application Kit, Apr. 2007, at 13, www.ojp.usdoj.gov/odp/docs/FY07_UASI_Guidance.pdf.

[321] *E.g.*, VA. CODE § 36-105.3, Security of certain records, http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+36-105.3.

[322] *E.g.*, VA. CODE § 44-146.22, Development of measures to prevent or reduce harmful consequences of disasters; disclosure of information, http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+44-146.22.

[323] *Cf.*, San Gabriel Tribune v. Superior Court, 143 Cal. App. 3d 762, 192 Cal. Rptr. 415 (Cal. App. 2d Dist. 1983) (public interest in monitoring city's contracting for services and regulation of contractors' fees charged to residents outweighs city's interest in not discouraging contractors from submitting proprietary information justifying need for rate increases) and Eskaton Monterey Hosp. v. Myers, 134 Cal. App. 3d 788, 184 Cal. Rptr. 840 (Cal. App. 3d Dist. 1982) (Public interest in preventing regulated businesses from circumventing effective compliance investigations by obtaining auditors' procedural manuals outweighs any public interest in disclosure).

[324] Florida Attorney General Advisory Legal Opinion AGO 2002-74 – Nov. 4, 2002, http://myfloridalegal.com/ago.nsf/Opinions/D4CFF22D8B492BDF85256C6700541A22 (accessed Apr. 1, 2009); Summary: http://brechner.org/reports/2002/12dec2002.pdf (accessed Apr. 1, 2009).

[325] *E.g.*, Blum v. N.Y. Stock Exchange, Inc., 263 A.D. 2d 522, 693 N.Y.S.2d 225 (N.Y.A.D. 2 Dept. 1999) (reasonable to require plaintiff in suit under New York State Human Rights Law (Executive Law § 290, *et seq*.) to execute confidentiality agreement before receiving documents regarding the security and evacuation routes of defendant, as defendant sufficiently demonstrated that documents sought by plaintiff involved sensitive security information which, if released to public, could jeopardize the safety of defendant's employees).

[326] For a review of state public records laws, *see* Burt Braverman and Wesley Heppler, *A Practical Review of State Open Records Laws*, 49 GEO. WASH. L. REV. 720 (1981).

sure, the applicability of disclosure requirements to contract documents, and penalties for violating disclosure requirements. This section touches on all of these issues. Specific exemptions are discussed in the following two sections.

In addition to state laws, public agencies may be subject to local public records requirements.[327] Generally, but not always, these ordinances rely on existing state law.[328]

1. Applicability to Transit Agencies

It is more likely than not that state disclosure requirements will apply to a public transit agency within the state. Many state public records laws make those laws applicable to all political subdivisions, as well as quasi-governmental agencies that receive public funds. Missouri, for example, includes in its definition of "public governmental body" not only political subdivisions but quasi-governmental bodies and bi-state development agencies.[329]

In addition, most states make public records requirements directly applicable to private entities under certain circumstances. Thus, depending on state law, even private contract providers of public transportation may be directly subject to open records requirements.[330]

2. Definition of Public Record

Generally, state law is likely to define "public record" rather broadly, although the specificity of the definition may vary from state to state. For example, Arizona defines "records" as follows:

> In this chapter, unless the context otherwise requires, "records" means all books, papers, maps, photographs or other documentary materials, regardless of physical form or characteristics, including prints or copies of such items produced or reproduced on film or electronic media pursuant to section 41-1348, made or received by any governmental agency in pursuance of law or in connection with the transaction of public business and preserved or appropriate for preservation by the agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the government, or because of the informational and historical value of data contained therein.[331]

The Arizona Supreme Court considers this to be a broad definition, but has held that in construing the meaning of "public records," documents must have a substantial nexus with the government agency's activities to be considered public records,[332] a standard that

---

[327] *E.g.*, San Francisco Sunshine Ordinance, § 67, www.sfgov.org/site/sunshine_page.asp?id=34495 (accessed Sept. 26, 2009).

[328] *Looking for Sunshine: Protecting Your Right to Know*, League of Women Voters, Jan. 2006, www.lwv.org/Content/ContentGroups/Projects/OpennessinGovernment/40404_LWV_LoRes.pdf (accessed Sept. 29, 2009).

[329] M.R.S. § 610.010 (4), http://ago.mo.gov/sunshinelaw/chapter610.htm#header1 provides:

> (4) "Public governmental body," any legislative, administrative or governmental entity created by the constitution or statutes of this state, by order or ordinance of any political subdivision or district, judicial entities when operating in an administrative capacity, or by executive order, including:
>
> ***
>
> (c) Any department or division of the state, of any political subdivision of the state, of any county or of any municipal government, school district or special purpose district including but not limited to sewer districts, water districts, and other subdistricts of any political subdivision;
>
> ***
>
> (f) Any quasi-public governmental body. The term "quasi-public governmental body" means any person, corporation or partnership organized or authorized to do business in this state pursuant to the provisions of chapter 352, 353, or 355, RSMo, or unincorporated association which either:
>
> a. Has as its primary purpose to enter into contracts with public governmental bodies, or to engage primarily in activities carried out pursuant to an agreement or agreements with public governmental bodies; or
>
> b. Performs a public function as evidenced by a statutorily based capacity to confer or otherwise advance, through approval, recommendation or other means, the allocation or issuance of tax credits, tax abatement, public debt, tax-exempt debt, rights of eminent domain, or the contracting of leaseback agreements on structures whose annualized payments commit public tax revenues; or any association that directly accepts the appropriation of money from a public governmental body, but only to the extent that a meeting, record, or vote relates to such appropriation; and
>
> (g) Any bi-state development agency established pursuant to section 70.370, RSMo.

[330] Craig D. Feiser, *Protecting the Public's Right to Know: The Debate Over Privatization and Access to Government Information Under State Law*, 27 FLA. STATE L. REV. 825, www.law.fsu.edu/Journals/lawreview/downloads/274/Feiser.pdf .

[331] ARIZ. REV. STAT. 41-1350. Definition of records, www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/41/01350.htm&Title=41&DocType=ARS. Definitions may be less specific and still cover a broad range of documents. For example, Alabama defines public records as follows:

> As used in this article, the term "public records" shall include all written, typed or printed books, papers, letters, documents and maps made or received in pursuance of law by the public officers of the state, counties, municipalities and other subdivisions of government in the transactions of public business and shall also include any record authorized to be made by any law of this state belonging or pertaining to any court of record or any other public record authorized by law or any paper, pleading, exhibit or other writing filed with, in or by any such court, office or officer.

ALA. CODE § 41-13-1, www.legislature.state.al.us/codeofalabama/1975/41-13-1.htm.

[332] Griffis v. Pinal County, 215 Ariz. 1, 156 P.3d 418, 421 (2007) (holding that mere possession of personal records by a government employee does not make the records public for purposes of disclosure requirements). *See* Lindsay J. Taylor, *Griffis v. Pinal County: Establishing When a Public Official's Personal Emails Are Public Records Subject to Disclosure*, 49 ARIZ. L. REV. 1027 (2007). The Colorado Supreme Court has taken a similar view of the status of public records under its state's law, which requires that public records be those that a public agency "made, maintained, or kept for use in exercise of functions required or authorized by law or administrative rule or involving the receipt or expenditure of public funds." Denver

should cover contracting documents. In contrast, the recently enacted Pennsylvania Right to Know Law presumes a record in the possession of a local agency to be a public record (subject to stated exemptions).[333]

The Washington Public Records Act defines "public record" as including "any writing containing information relating to the conduct of government or the performance of any governmental or proprietary function prepared, owned, used, or retained by any state or local agency regardless of physical form or characteristics."[334] The Washington Supreme Court has held that information "applied to a given purpose or instrumental to an end or process" is "used" under this definition, so that where there is a connection between the information and the agency's decision-making process, "evaluation, and reference to information constitutes 'use' and, therefore, qualifies such information as a public record."[335] The *Concerned Ratepayers* court found that the information at issue came under this definition, despite the fact that the agency did not possess or use the information in its final work product.[336]

State statutes vary on whether they address electronic records. The absence of specific provisions may leave the status of electronic records under disclosure statutes unclear.[337] In addition, the assessment of what constitutes a public record may be complicated by the proliferation of electronic record keeping and software that allows collaborative access as well as document management capabilities. Where it is clear that electronic records are covered, ancillary documents such as emails can be considered public records. State law may require that the content of such electronic documents have the requisite nexus to public business.[338] For example, a Wisconsin court examined the status of an email concerning city business that was sent from a private citizen to a public official. The court found that having the email discussed by the official at a public meeting provided the necessary nexus, with disclosure requirements extending to the meta data as well as the body of the email.[339]

State law may specify whether contractors' records are subject to the state public records requirements. For example, Pennsylvania law specifically subjects to the Right to Know Law public records in the possession of a contractor performing a government function for a local agency.[340] Wisconsin law requires a state authority to make records produced or collected under contract with the authority (except for specified personally identifiable information) publicly available to the same extent as if the records were maintained by the authority.[341] Accordingly, under Wisconsin law a state authority may not avoid public records requirements by delegating a record's creation and custody to an agent.[342] While this specific provision does not apply to local agencies in Wisconsin, similar requirements in other jurisdictions may apply to local agencies or to state-level transit agencies.

A related issue is the status of documents that are not, strictly speaking, contracts, but are related to contract documents. The Pennsylvania Right to Know Law specifically includes a contract dealing with receipt or disbursement of funds by any agency in the definition of public record,[343] with the requester of information bearing the burden of establishing that particular documents indeed fall within that definition.[344] The Pennsylvania Supreme Court has held that documents that are not facially classified as contracts may nonetheless be held to be public records "where the information requested was sufficiently connected to or closely related to these statutory categories."[345]

Where state statutes do not clearly address under public records acts the status of records created by contractors, courts will look to the facts of the case, including whether the records are in the possession of or under the control of the public agency. For example, the Arkansas Supreme Court has suggested that documents may be under the administrative control of a

---

Publishing Co. v. County Comm. of Arapahoe, 121 P.3d 190, 191 (Col. 2005) (simple possession, creation, or receipt of email record by public official or employee not dispositive as to whether the record is "public record;" inquiry must be content-driven).

[333] Section 305, Act 3 of 2008, Right to Know Law, www.dced.state.pa.us/public/oor/pa_righttoknowlaw.pdf.

[334] WASH. REV. CODE 42.56.010, Definitions, http://apps.leg.wa.gov/rcw/default.aspx?cite=42.56.010.

[335] Concerned Ratepayers Ass'n v. Pub. Utility Dist. No. 1 of Clark County, Wash., 138 Wash. 2d 950, 983 P.2d 635, 637 (1999). The court refers to WASH. REV. CODE 42.17.020(36), the predecessor provision to WASH. REV. CODE 42.56.010, which is substantively the same provision.

[336] *Id*. at 640–42.

[337] *See* Leanne Holcomb & James Isaac, *Wisconsin's Public-Records Law: Preserving the Presumption of Complete Public Access in the Age of Electronic Records*, 2008 WIS. L. REV. 515, 517 (2008). The authors argue that deleted emails and other electronic documents should be treated as public records subject to disclosure.

[338] *See* Griffis, 156 P.3d 418. The GAO has discussed the public records challenge of managing email at the federal level. U.S. GOV'T ACCOUNTABILITY OFFICE, FEDERAL RECORDS, AGENCIES FACE CHALLENGES IN MANAGING E-MAIL (2008), www.gao.gov/new.items/d08699t.pdf.

[339] O'Neill v. City of Shoreline, 145 Wash. App. 913, 187 P.3d 822 (2008).

[340] Section 506(d), Act 3 of 2008, Right to Know Law, www.dced.state.pa.us/public/oor/pa_righttoknowlaw.pdf.

[341] WIS. STAT. § 19.36(3), www.legis.state.wi.us/statutes/Stat0019.pdf.

[342] Journal/Sentinel, Inc. v. Sch. Bd. of Sch. Dist. of Shorewood, 186 Wis. 2d 443, 521 N.W.2d 165 (Wis. App. 1994).

[343] 65 PA. STAT. § 66.1.

[344] State Univ. v. State Employees' Ret. Bd., 880 A.2d 757, 763 (Pa. Cmwlth. 2005), citing LaValle v. Office of General Counsel, 564 Pa. 482, 769 A.2d 449 (2001).

[345] *Id*. at 764 (Pa. Cmwlth. 2005), citing LaValle v. Office of Gen. Counsel, 564 Pa. 482, 493–94, 769 A.2d 449, 456 (2001) and North Hills News Record v. Town of McCandless, 555 Pa. 51, 722 A.2d 1037 (1999).

state agency even if they are in physical possession of a private contractor, making the documents public records under that state's FOIA.[346] The court stated that it "will not permit the circumvention of the FOIA by the simple 'handoff' of documents to entities not covered by the Act."[347]

3. Presumption of Disclosure

Some state statutes explicitly provide that they are to be construed as providing for disclosure. For example, Maryland's Public Information Act state law requires that the statute "be construed in favor of permitting inspection of a record."[348] Other statutory language that is generally construed as creating a presumption of disclosure includes language that provides a right to inspect all public records unless otherwise exempted and language that places on the government agency the burden of establishing the appropriateness of asserting an exemption. For example, Alabama's statute providing its citizens the right to inspect and copy any public writing unless otherwise expressly provided by statute[349] has been interpreted to constitute a presumption in favor of public disclosure.[350] Similarly, under New York's Freedom of Information Law, the requirement of making all agency records available, except to the extent exempted, is construed as creating a presumption of access.[351]

The presumption of disclosure may be the basis for a requirement to segregate exempt and nonexempt information.[352] State law may require that where an agency has identified an applicable exemption, the agency review the record to determine whether the exempt portions can reasonably be excised; if so, the agency must redact the exempt portion(s) and disclose the rest of the record. States that expressly require segregation include Hawaii,[353] Idaho,[354] Nebraska,[355] New Mexico,[356] North Dakota,[357] Oklahoma,[358] Oregon,[359] and Wisconsin.[360] In addition to requiring segregation, the Missouri statute requires agencies to design public records to facilitate segregation to the extent practicable.[361] The issue may also be addressed indirectly, as under the North Carolina statue providing that commingling of confidential and nonconfidential information is not a valid basis for refusing to provide information.[362]

4. Approach to Exemptions

Generally state laws provide that public disclosure exemptions are to be narrowly construed. Examples include Arkansas,[363] Kentucky,[364] Massachusetts,[365] Missouri,[366] Nevada,[367] and Washington.[368] Strict construction may prohibit courts from going beyond statutory language to create exemptions. For example, the Dis-

---

[346] ARK. CODE ANN. §§ 2519101–2519109 (Repl. 2002 & Supp. 2005).

[347] Nabholz Constr. Corp. v. Contractors for Public Prot. Ass'n, 371 Ark. 411, 266 S.W.3d 689 (2007).

[348] Public Information Act, § 10-612(b). *See Maryland Public Information Act Manual*, ch. III, Exceptions to Disclosure (11th ed. 2008), www.oag.state.md.us/Opengov/pia.htm.

[349] ALA. CODE, § 36-12-40.

[350] Chambers v. Birmingham News Co., 552 So. 2d 854, 856 (Ala. 1989).

[351] Matter of Citizens for Alternatives to Animal Labs v. Bd. of Trustees of State Univ. of N.Y., 92 N.Y.2d 357, 703 N.E.2d 1218, 681 N.Y.S.2d 205 (1998); Committee on Open Government, FOIL-AO-14554, Mar. 5, 2004, www.dos.state.ny.us/COOG/ftext/f14554.htm.

[352] Committee on Open Government, FOIL-AO-14554, Mar. 5, 2004, *citing* Gould v. N.Y. City Police, 89 NY.2d 267, 276 (1996), www.dos.state.ny.us/COOG/ftext/f14554.htm.

[353] The Uniform Information Practices Act (Modified), at 36, 40-41, www.state.hi.us/oip/UIPA%20Manual%205aug08.pdf.

[354] IDAHO CODE § 9-341, www.legislature.idaho.govidstat/Title9/T9CH3SECT9-341.htm.

[355] NEB. REV. STAT. § 84-712.06, http://uniweb.legislature.ne.gov/laws/statutes.php?statute=s8407012006.

[356] Section 14-2-9(A), NMSA, www.conwaygreene.com/nmsu/lpext.dll?f=templates&fn=main-h.htm&2.0.

[357] 2004 N.D. Op. Atty. Gen. Open Records and Meetings Opinion 2004-O-23, citing N.D. CENT. CODE § 44-04-18.10, www.ag.nd.gov/Opinions/2004/OR/2004-O-23.pdf.

[358] 51 OKLA. STAT. SUPP. 2005 § 24A.5.2, www.lsb.state.ok.us/osstatuestitle.html.

[359] OR. REV. STAT. 192.505, www.leg.state.or.us/ors/192.html.

[360] WIS. STAT. § 19.36(6), www.legis.state.wi.us/statutes/Stat0019.pdf.

[361] MO. REV. STAT. § 610.024. Public record containing exempt and nonexempt materials, nonexempt to be made available—deleted exempt materials to be explained, exception, http://ago.mo.gov/sunshinelaw/chapter610.htm#header8.

[362] N.C. GEN. STAT. § 132[ ]6(c), www.ncleg.net/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_132.html.

[363] Orsini v. State, 340 Ark. 665, 13 S.W.3d 167 (2000) (court narrowly construes exemptions "to counterbalance the self-protective instincts of the government bureaucracy.").

[364] KY. REV. STAT. 61.871, Policy of KY. REV. STAT. 61.870 to 61.884—Strict construction of exceptions of KY. REV. STAT. 61.878. (Strict construction of exceptions required "even though such examination may cause inconvenience or embarrassment to public officials or others."), www.lrc.ky.gov/KRS/061-00/871.PDF.

[365] Attorney General v. Assistant Comm'r of the Real Property Dep't of Boston, 380 Mass. 623, 625, 404 N.E.2d 1254, 1255–1256 (1980).

[366] MO. REV. STAT. § 610.011. Liberal construction of law to be public policy, http://ago.mo.gov/sunshinelaw/chapter610.htm#header2.

[367] NEV. REV. STAT. 239.001, www.leg.state.nv.us/NRS/NRS-239.html#NRS239Sec001.

[368] WASH. REV. CODE 42.56.030, http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.030.

trict of Columbia strictly construes its exemptions and does not allow judicially-created exemptions.[369]

State courts may prohibit blanket assertions of exemptions. For example, New York requires that the agency demonstrate the applicability of the exemption by "articulating a particularized and specific justification for denying access."[370] The New York court requires that a record fit precisely within the cited exemption to be withheld.[371] Arkansas takes the same approach, requiring a record that does not fall clearly within an exemption to be disclosed.[372]

State laws vary as to whether an applicable exemption precludes disclosure or merely provides a basis for denying disclosure. Arkansas, for one, requires agencies to withhold information that falls within an exemption, except under court order, subpoena, or written consent of the person protected by the exemption.[373] States whose exemptions are deemed to be discretionary include Hawaii,[374] Michigan,[375] New York,[376] and South Carolina.[377] Nebraska's statute sets forth categories of records that may be withheld at the discretion of the lawful custodian unless they are publicly disclosed in open court, open administrative proceeding, or open meeting or are disclosed by a public agency pursuant to its duties.[378] The District of Columbia statute provides that exemptions do not apply if disclosure of information is authorized or mandated by other law.[379]

State laws may include a general exemption that specifically calls for balancing the public interest in favor of disclosure against the public interest in favor of nondisclosure. For example, California's Public Records Act allows an agency to withhold information "by demonstrating that…on the facts of the particular case the public interest served by not disclosing the record clearly outweighs the public interest served by disclosure of the record."[380] Absent a provision explicitly requiring a balancing of public interests, the state court may take the position that an exemption requires no balancing beyond the language of the exemption.[381]

5. Burden of Proof re Classification of Information as Exempt from Disclosure

Under Federal FOIA, the agency asserting the exemption bears the burden of proving that the requested information falls within the exemption. States that similarly place the burden on the government agency that seeks to assert an exemption include Arkansas,[382] California,[383] Connecticut,[384] Hawaii,[385] Nevada,[386] New York,[387] Rhode Island,[388] and Washington.[389] The burden is generally required to be met with a specific showing, rather than conclusory claims.[390] At least two states employ a preponderance of the evidence standard.[391]

---

[369] D.C. CODE ANN. § 2-534(b); Barry v. Wash. Post Co., 529 A.2d 319, 321 (D.C. 1987).

[370] Capital Newspapers Div. of Hearst Corp. v. Burns, 67 N.Y.2d 562, 566, 496 N.E.2d 665, 667, 505 N.Y.S.2d 576, 578 (1986).

[371] Matter of Fink v. Lefkowitz, 47 N.Y.2d, 567, 571, 393 N.E.2d 463, 465, 419 N.Y.S.2d 467, 471 (1979); Data Tree, LLC v. Romaine, 9 N.Y.3d 454, 880 N.E.2d 10, 849 N.Y.S.2d 489 (2007).

[372] *E.g.*, Orsini, 340 Ark. 665.

[373] Ark. Op. Att'y Gen. Nos. 99-334, 91-374, 91-323.

[374] The Uniform Information Practices Act (Modified), at 34, www.state.hi.us/oip/UIPA%20Manual%205aug08.pdf.

[375] Tobin v. Mich. Civil Serv. Comm'n, 98 Mich. App. 604, 296 N.W.2d 320 (1980).

[376] Capital Newspaper v. Burris, 67 N.Y.2d 562, 496 N.E.2d 665, 505 N.Y.S.2d 576 (1986).

[377] S.C. CODE ANN. § 30-4-40, www.scstatehouse.gov/code/t30c004.htm.

[378] NEB. REV. STAT. § 84-712.05, http://nebraskalegislature.gov/laws/laws-index/chap84-full.html.

[379] Dunhill v. Dir., D.C. Dep't of Transp., 416 A.2d 244 (D.C. 1980).

[380] CAL. GOV'T CODE § 6255, subd.(a). *Cf.*, Washington's Public Disclosure Act, ch. 42.17, WASH. REV. CODE, held not to contain any general exemption. Progressive Animal Welfare Society (PAWS) v. The Univ. of Wash., 125 Wash. 2d 243, 884 P.2d 592 (1994).

[381] *E.g.*, Dir., Dep't of Information v. Freedom Comm'n, 274 Conn. 179, 192, 874 A.2d 785, 793 (Conn. 2005) (no separate balancing of public interest required under exemption for records where there is reasonable basis to believe disclosure may result in safety risk).

[382] Orsini, 340 Ark. 665.

[383] Michaelis, 44 Cal. Rptr. 3d at 667 (citation omitted).

[384] FOIA Comm., 874 A.2d 785. A town's director of information technology refused a request for copies of computerized data from a town's geographic information system based on several exemptions including Conn. Gen. Stat. § 1-210(b)(19). The appellate court held that the IT director failed to meet his burden of seeking a determination from the commissioner of public works that the GIS information fell under the public safety exception, and so affirmed the earlier decisions requiring disclosure. *Id*. at 189.

[385] HAW. REV. STAT. § 92F-15(c), www.state.hi.us/oip/uipa.html#92F15.

[386] NEV. REV. STAT. 239.0113, Burden of proof where confidentiality of public book or record is at issue, www.leg.state.nv.us/NRS/NRS-239.html#NRS239Sec0113.

[387] Fink, 47 N.Y.2d 567; Data Tree, 880 N.E.2d 10.

[388] Section 38-2-10, www.rilin.state.ri.us/statutes/title38/38-2/38-2-10.HTM.

[389] WASH. REV. CODE 42.56.550, http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.550. *See* Rental Housing Ass'n v. City of Des Moines, 199 P.3d 393, 165 Wash. 2d 525 (Wash. 2009).

[390] *E.g.*, Trombley v. Bellows Falls Union High Sch. Dist., 160 Vt. 101, 624 A.2d 857 (1993).

[391] Nevada: NEV. REV. STAT. 239.0113, Burden of proof where confidentiality of public book or record is at issue, www.leg.state.nv.us/NRS/NRS-239.html#NRS239Sec0113; Virginia: Virginia Freedom of Information Act, VA. CODE ANN. § 2.2-3713(E), http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-3713.

6. Applicability to Contract Documents

As noted, *supra*, contract documents are likely to come within the definition of public record, particularly those documents within a transit agency's possession. Interests in protecting contract information may shift between the time bids are submitted and the time bidding is closed.[392] However, for the most part this distinction runs to protecting the government interest in preserving competition, rather than being applicable to security information. For example, in Hawaii, the general exemption under the Uniform Information Practices Act for information that must be confidential to protect legitimate government functions has been interpreted to apply to information that "if disclosed, would raise the cost of government procurements or give a manifestly unfair advantage to any person proposing to enter into a contract or agreement with an agency." Hawaii's Attorney General has applied this interpretation to find that before bid submission an agency may withhold the identity of persons that have picked up or received bid solicitations, attended a bidder's conference, or submitted a notice of intent to bid or bid itself; after bid submission the information must be made publicly available.[393] Vermont also protects records of contract negotiations.[394]

Even after the contractor has been selected, information may be protectable until the contract is finalized.[395] Again, this requirement goes to protecting the government's competitive position, rather than protecting security information.

7. Penalties for Violations/Attorney Fees

State law may provide penalties for violating open records act provisions. Generally these provisions apply to negligent or willful violations. The severity of penalties for violations varies. For example, Kansas public agencies that knowingly violate provisions of the Open Records Act may be subject to civil penalties, up to $500 per violation.[396] Maine law provides for similar penalties.[397] Minnesota's statute provides for larger civil penalties and makes willful violation of the Government Data Act a misdemeanor and just cause for suspension without pay or dismissal of a public employee.[398] Missouri provides for civil penalties against public governmental bodies and members of public governmental bodies who willfully violate the Sunshine Law and for the removal and fining or jailing of public officials who violate the Public Records Act.[399] Nebraska provides for similar penalties for officials who violate the open records provisions, and provides equitable remedies for citizens who seek to enforce the public records provisions, including attorneys fees and other litigation costs for citizens who substantially prevail.[400] West Virginia makes willful violation of the state Freedom of Information chapter a misdemeanor punishable by fine and/or imprisonment.[401] Wisconsin allows both actual and punitive damages for willfully delaying release of information, as well as allowing forfeitures up to $1,000 for arbitrary and capricious denial or delay of requests for information.[402] Depending on the structure of state law, such penalties may also apply to violation of records management statutes.[403]

---

[392] *E.g.*, FLA. STAT. § 119.071(1)(b) [protection of sealed bids and competitive negotiations until decision made]. www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0119/SEC071.HTM&Title=-%3E2008-%3ECh0119-%3ESection%20071#0119.071; FLA. STAT. § 337.168, Confidentiality of official estimates, identities of potential bidders, and bid analysis and monitoring system, www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0337/SEC168.HTM&Title=-%3E2008-%3ECh0337-%3ESection%20168; N.Y.S. Committee on Open Government opinion, Aug. 2, 1993, letter to City Attorney of City of North Tonawanda, www.dos.state.ny.us/coog/ftext/f7837.htm (accessed Mar. 31, 2009).

[393] Dec. 15, 1994, letter from Office of Information Practices, Department of Attorney General to State Procurement Office, www.state.hi.us/oip/opinionletters/opinion%2094-26.PDF (accessed Aug. 10, 2009).

[394] 1 VT. STAT. ANN. § 317(c)(15), Records of contract negotiations (1976). *See* Legislative Council Staff Report on Public Records Requirements in Vermont, Jan. 2007, www.leg.state.vt.us/REPORTS/07PublicRecords/Public%20Records%20Requirements%20in%20Vermont.pdf (accessed Sept. 20, 2009).

[395] N.Y.S. Committee on Open Government opinion, Jan. 31, 2000, FOIL-AO-11933, www.dos.state.ny.us/coog/ftext/f11933.htm (accessed Mar. 31, 2009).

[396] KAN. STAT. ANN., 45-223, Civil penalties for violations, Accessible from www.kslegislature.org/legsrv-statutes/index.do.

[397] ME. REV. STAT. ANN. § 410, Violations, www.mainelegislature.org/legis/statutes/1/title1sec410.html.

[398] MINN. STAT. § 13.08, www.revisor.leg.state.mn.us/statutes/?id=13.08; MINN. STAT. § 13.09, www.revisor.leg.state.mn.us/statutes/?id=13.09.

[399] MO. REV. STAT. § 610.027, Violations—remedies, procedure, penalty—validity of actions by governing bodies in violation—governmental bodies may seek interpretation of law, attorney general to provide. http://ago.mo.gov/sunshinelaw/chapter610.htm#header11; MO. REV. STAT. § 109.180, www.moga.mo.gov/statutes/C100-199/1090000180.HTM.

[400] NEB. REV. STAT. § 84-712.09, http://uniweb.legislature.ne.gov/laws/statutes.php?statute=s8407012009; NEB. REV. STAT. § 84-712.09, http://uniweb.legislature.ne.gov/laws/statutes.php?statute=s8407012007.

[401] W.VA. CODE § 29B-1-6, www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=29b.

[402] WIS. STAT. § 19.37, www.legis.state.wi.us/statutes/Stat0019.pdf.

[403] *E.g.,* LA. REV. STAT. § 44-37, Penalties for violation by custodians of records, www.legis.state.la.us/lss/lss.asp?doc=99714.

Although state statutes may specify the penalty, transit agencies may have to look to the case law to determine how those penalties are applied. For example, in Washington, the open records law provides for a penalty ranging from $5 to $100 per day that a record is improperly withheld.[404] The Washington Supreme Court has held that the penalties need not be assessed per record and that trial courts must assess a penalty for each day a record is withheld.[405] The state court has set forth the factors—both mitigating and aggravating—that a trial court should consider in setting penalties.[406]

State public records acts may provide for attorney fees for the prevailing party.[407] A California court has held that under the California Public Records Act the requesting party need not receive all requested documents to prevail: where the requesting party received one of two requested documents—without question only because of the lawsuit—and the claim for the document not disclosed was not frivolous, the requesting party had prevailed.[408]

B. Public Records Laws—Security Exemptions[409]

There are various types of security exemptions, many of which have been adopted since 9/11.[410] It is not uncommon for security exemptions to exclude the disclosure of information related to structural or environmental problems in buildings or information connected to inquiries conducted after the occurrence of catastrophic events.[411] The discussion of examples of types of security exemptions is intended to provide context for transit agencies in developing their own security policies.

Some states directly address the issue of protection of CII/SSI, although not necessarily specifically in the context of transportation. For example, Arizona's public records law provides: "Nothing in this chapter requires the disclosure of a risk assessment that is performed by or on behalf of a federal agency to evaluate critical energy, water or telecommunications infrastructure to determine its vulnerability to sabotage or attack."[412] The statutory construction argument could be made that because such statutes specifically protect other infrastructure but not transportation infrastructure, that transportation infrastructure is not protected. However, we are not aware of any decisions to that effect.

State security exemptions may also explicitly address providing contractor access to exempted information. For example, Florida's security exemption for building plans and blueprints specifically provides that the exempt security information may be disclosed to "a licensed architect, engineer, or contractor who is performing work on or related to the building, arena, stadium, water treatment facility, or other structure owned or operated by an agency."[413] However, it is not clear whether the disclosure provision applies to contractors at the bidding stage. The language in the Missouri state statute is arguably more expansive: "Nothing in this exception shall be deemed to close information regarding expenditures, purchases, or contracts made by an agency in implementing these guidelines or policies."[414] This language takes expenditure, purchase, and contract information out of the security exemption.

It is not yet apparent to what extent state security exemptions have been used to protect security information. For example, in 2007, the Maryland Office of the Attorney General (OAG) submitted a report to the Maryland Governor and General Assembly on the public security exception added in 2002 to Maryland's Public Information Act. The OAG reported that the exception had rarely been asserted to deny a public records request and there had been no reported (and apparently no unreported) cases applying the exception. Nonetheless, the OAG recommended that the exception be retained without modification.[415] The OAG found that two agencies had decided not to invoke the security exemptions after the requesters agreed to conditions: in one case, not making a copy of the requested information

[404] WASH. REV. CODE 42.56.550(4).

[405] Yousoufian v. Ron Sims, 152 Wash. 2d 421, 425, 98 P.3d 463, 465 (2004).

[406] Yousoufian v. Ron Sims, 165 Wash. 2d 439, 200 P.3d 232 (2009).

[407] *E.g.*, Arizona: ARIZ. REV. STAT. § 39-121.02(B) (Supp. 2006) (attorneys' fees may be awarded if the person seeking public records substantially prevails); California Public Records Act, Government Code, § 6259(d) (court costs and reasonable attorney fees to plaintiff should plaintiff prevail; court costs and reasonable attorney fees to public agency if court finds plaintiff's case is clearly frivolous).

[408] L.A. Times v. Alameda Corridor Transp. Auth., 107 Cal. Rptr. 2d 29, 88 Cal. App. 4th 1381 (Cal. Ct. App. 2d Dist. 2001).

[409] *See* Cathy Atkins and Larry Morandi, Protecting Water System Security Information, Sept. 2003 discussion of National Conference of State Legislatures, Description of FOIA Exemptions, *available at* http://www.oe.netl.doe.gov/documents/Water_Security.pdf.

[410] *Right to Know vs. Need to Know: States Are Re-examining Their Public-Records Laws in the Wake of Sept. 11*, Homeland Security Brief, The Council of State Governments, Dec. 2003, www.csg.org/pubs/Documents/Brief1003RightToKnow.pdf (accessed Sept. 20, 2009).

[411] *E.g.*, Virginia: VA. CODE § 2.2-3705.02, Exclusions to application of chapter; records relating to public safety, http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-3705.2.

[412] ARIZ. REV. STAT. 39-126, Federal risk assessments of infrastructure; confidentiality, www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/39/00126.htm&Title=39&DocType=ARS.

[413] FLA. STAT. § 119.071(3)(b)3.b, www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0119/SEC071.HTM&Title=-%3E2008-%3ECh0119-%3ESection%20071#0119.071. Building plans and blueprints are protected under this exemption if they depict internal layout and structural elements of structures owned or operated by government agencies.

[414] MO. REV. STAT. § 610.021(18), http://ago.mo.gov/sunshinelaw/chapter610.htm#header7.

[415] GANSLER, *supra* note 53.

and in the other, undergoing a background check before receiving the information.[416] The OAG found that the language in the security exception—that authorizing the custodian to deny inspection "only to the extent" that disclosure would threaten public security as specified under the statute—allowed what would otherwise be unauthorized conditions on disclosure. The OAG noted that even without this exception, federal statutes such as the CIIA would preclude disclosing certain information under the Act because the general rule of access under the Act is "unless otherwise provided by law."[417]

This section provides examples of the types of security exemptions that states have enacted. The intent is to provide context to assist transit agencies in analyzing the specific exemptions under their own state law. A state-by-state list of security exemptions is included as Appendix C, *infra*.

1. Endanger Life or Safety

New York's Freedom of Information Law (FOIL) allows an agency to deny access to information disclosure that could "endanger the life or safety of any person."[418] In response to a requester who had been denied access to information concerning security deployment at a county event, the agency that provides opinions on FOIL stated that the detail requested should have some bearing on whether information should be subject to this exception. The committee provided this example:

> For instance, there is unquestionably an interest in ensuring a safe supply of water for the public, and proposals have been made, primarily in other jurisdictions, to require that maps indicating the location of water supplies be kept confidential. That kind of proposal is, in my view, overly broad and largely unenforceable. I can see the Hudson River from my office, and Reservoir Road is likely close to a reservoir. Maps that can purchased [sic] at any number of locations contain information of that nature. On the other hand, if a map is so detailed that it indicates the location of certain valves, places where terrorists or others could deposit poisons or chemical or biological agents, perhaps it could be contended that there is a reasonable likelihood that disclosure, due to the degree of detail, could endanger life or safety.[419]

The committee went on to note that while information about specific deployment of security personnel might arguably endanger life or safety, information about the number of participating officers and their functions was too minimally detailed to be likely to endanger life or safety.[420]

2. Vulnerability Assessments

As discussed above, Maryland's Public Information Act allows a record custodian to deny inspection of part of a specified public record based on a belief that inspection would be contrary to the public interest. Specified records include response procedures or plans that would reveal vulnerability assessments and

> building plans, blueprints, schematic drawings, diagrams, operational manuals, or other records of airports and other mass transit facilities…the disclosure of which would reveal the building's, structure's or facility's internal layout, specific location, life, safety, and support systems, structural elements, surveillance techniques, alarm or security systems or technologies, operational and transportation plans or protocols, or personnel deployments.

However, inspection may only be denied to the extent that inspection would jeopardize facility security, facilitate planning of a terrorist attack, or endanger life or physical safety.[421]

Texas law more broadly protects vulnerability assessments. Texas's Public Information Act excepts from disclosure "information considered to be confidential by law, either constitutional, statutory, or by judicial decision."[422] The Texas Homeland Security Act in turn makes information confidential if it

> (1) is collected, assembled, or maintained by or for a governmental entity for the purpose of preventing, detecting, or investigating an act of terrorism or related criminal activity; and
>
> (2) relates to an assessment by or for a governmental entity, or an assessment that is maintained by a governmental entity, of the risk or vulnerability of persons or property, including critical infrastructure, to an act of terrorism or related criminal activity.[423]

The Texas Attorney General has advised that merely because information relates to security concerns does not make it confidential. Rather, if a governmental body asserts information is excepted from disclosure under the Public Information Act due to the security provisions of the Homeland Security Act, the body must adequately explain how the requested information falls within the scope of the claimed provision. The Attorney General found that information described as being used to "evaluate information about potential threat elements in [various Texas] jurisdictions" and "determine equipment, training, exercise, planning, organizational and technical needs" and forwarded to DHS to determine funding needs appropriately falls within the scope

---

[416] *Id.* at 7–8.

[417] *Id.* at 10. The OAG cited 6 U.S.C. § 133(a)(1)(E) as an example of a federal statute precluding disclosure of information despite the PIA's general presumption of disclosure.

[418] Freedom of Information Law, N.Y. PUB. OFF. § 87(2)(f).

[419] *See* N.Y.S. Committee on Open Government opinion, FOIL-AO-16715, Aug. 6, 2007, www.dos.state.ny.us/coog/ftext/f16715.htm (accessed Mar. 31, 2009).

[420] *Id.*

[421] MD. CODE, § 10-618(b), Permissible denials: *Denial of inspection.*

[422] TEX. GOV'T CODE, § 552.101, Exception: Confidential Information, www.statutes.legis.state.tx.us/SOTWDocs/GV/pdf/GV.552.pdf.

[423] TEX. GOV'T CODE, § 418.177, Confidentiality of Certain Information Relating to Risk or Vulnerability Assessment, www.statutes.legis.state.tx.us/SOTWDocs/GV/pdf/GV.418.pdf.

of the cited provision of the Homeland Security Act; such information was required to be withheld.[424]

3. Other

As noted above, Maryland covers plans of mass transit facilities under its security exemption. Virginia also covers such plans to the extent they reveal the location or operation of "security equipment and systems, elevators, ventilation, fire protection, emergency, electrical, telecommunications or utility equipment and systems of any public building" or "operational and transportation plans or protocols, to the extent such disclosure would jeopardize the security of any governmental facility, building or structure or the safety of persons using such facility, building or structure."[425] The Virginia provision also covers training manuals, the disclosure of which would jeopardize public safety as specified under the statute.[426] Under the Virginia statute the record custodian need not, but may, disclose such information, except where prohibited by law.

Both Florida and Missouri exempt plans for security systems from mandatory disclosure.[427] The Florida statute includes threat assessments and threat response plans in its definition of "security system plan." However, the Missouri statute specifies: "Records related to the procurement of or expenditures relating to security systems purchased with public funds shall be open."[428]

C. Public Records Laws—Other Exemptions That May Protect SSI and Other Security Information

As noted in the discussion of the Federal FOIA, *supra*, a number of sunshine act exemptions that are not focused on security may be used to protect security information. These include general public interest exemptions, exemptions mandated by other statutes, trade secret and commercial information exemptions, and intra/inter agency memoranda exemptions.

1. General Public Interest

Hawaii's Uniform Information Practices Act contains an exception for information whose disclosure would frustrate a legitimate government function.[429] In 2007 Hawaii's Office of Information Practices (OIP) interpreted this as justifying the nondisclosure of information about the physical security of Hawaii's critical energy infrastructure submitted by private companies to Hawaii's Department of Business, Economic Development and Tourism (DBEDT).[430]

OIP examined the function of the agency in question, which was to ensure Hawaii's energy security. DBEDT argued that disclosing the requested information would expose the infrastructure to physical damage, thereby impairing its physical security and thus frustrating DBEDT's function. OIP looked to the use of FOIA's national security exemption to protect information about the physical security of nuclear power facilities, finding DBEDT's argument to be analogous. OIP found it unnecessary for information to be classified to be withheld at the state level. Rather "where an agency seeks to withhold information in the interest of public security, the agency must show that public disclosure of the information could reasonably be expected to cause damage to public security."

In contrast, in *Progressive Animal Welfare Soc. v. University of Washington (PAWS)*,[431] a seminal Washington State public records case, Washington's Supreme Court took the position that the state legislature had rejected the idea of a general "vital government functions" exemption.[432] The court also rejected the argument that Revised Code of Washington 42.17.330 provides such a general exemption.[433]

California's Public Records Act explicitly allows a government agency to withhold records "if it can demonstrate that, on the facts of a particular case, the public interest served by withholding the records clearly outweighs the public interest served by disclosure."[434] Under this exemption, there is a case-by-case balancing process "with the burden of proof on the proponent of nondisclosure to demonstrate a clear overbalance on the side of confidentiality."[435] California case law directs courts to look at the nature of the government activity being examined and how well the requested information would illuminate that activity.

In *County of Santa Clara*, a case involving a request for the county's GIS Basemap, the court found that

---

[424] Op. Tex. Att'y Gen. No. GA-7401 (2005), www.oag.state.tx.us/opinions/openrecords/50abbott/orl/2005/pdf/or200507401.pdf.

[425] VA. CODE, § 2.2-3705.2, Exclusions to application of chapter; records relating to public safety, Exclusions 4 and 6, http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-3705.2.

[426] *E.g.*, VA. CODE, § 2.2-3705.2, Exclusions to application of chapter; records relating to public safety, Exclusions 4 and 6.

[427] FLA. STAT. § 119.071(3)(a)2: A "security system plan" is exempt and confidential under the Florida public records law, www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0119/SEC071.HTM&Title=-%3E2008-%3ECh0119-%3ESection%20071#0119.071; MO. REV. STAT. § 610.021(19), http://ago.mo.gov/sunshinelaw/chapter610.htm#header7.

[428] MO. REV. STAT. § 610.021(19)(a), http://ago.mo.gov/sunshinelaw/chapter610.htm#header7.

[429] Uniform Information Practices Act, HAW. REV. STAT. § 92F-13(3) (1993), www.state.hi.us/oip/uipa.html#92F13.

[430] OIP Op. Ltr. No. 07-05, www.state.hi.us/oip/opinionletters/opinion%2007-05.pdf (accessed June 4, 2009).

[431] Progressive Animal Welfare Soc. v. Univ. of Wash., 125 Wash. 2d 243, 261, 884 P.2d 592, 601 (Wash. 1994), *citing* Laws of 1987, ch. 403, § 1, at 1546.

[432] *Id*. at 258–59, *citing* Laws of 1987, ch. 403, § 1, at 1546.

[433] *Id*. at 260–61.

[434] 170 Cal. App. 4th 1301, 1321, 89 Cal. Rptr. 3d 374, 388 (citation omitted) (discussing § 6255 of CPRA).

[435] *Id*., *citing* Michaelis, Montanari & Johnson v. Superior Court (2006), 38 Cal. 4th 1065, 1071, 44 Cal. Rptr. 3d 663, 136 P.3d 194.

there was a significant public interest in disclosure of the government activities at issue; the requested GIS Basemap would illuminate those activities; and the availability of other means to obtain the information—particularly given the lack of privacy concerns—did not prevent requiring disclosure under the Public Records Act. Finding that the public interest in disclosure was neither hypothetical nor minimal, the court then assessed the public interest in nondisclosure. The court rejected the county's argument that the GIS Basemap contained sensitive information that is not publicly available and that could not be easily segregated. The example cited by the county was the exact location of Hetch Hetchy reservoir components, which could be combined with publicly available information to allow terrorists to pinpoint the water lines and attack the San Francisco water system. The plaintiff's GIS expert, however, testified that in fact the GIS Basemap showed the water easements, not the sensitive water line locations, and that even the easement information could be easily segregated. The trial court had found that some of the information in the record requested had nothing to do with security, and that that information could not be "cloaked with the protection of CII/PCII simply by submission to OHS [the California Office of Homeland Security]." The appellate court agreed.[436]

States may also recognize a public interest exemption as a matter of common law. Wisconsin, for example, recognizes public interest exemptions, including a public interest balancing test that has been incorporated into state statute.[437] Attorney work product is another example of a common law exemption,[438] although one that may be incorporated into statutory exemptions as well.[439]

2. When Mandated by Federal or Other State Statutes

Most state public records statutes have provisions analogous to Federal Exemption 3, requiring that information be withheld if mandated by federal or other state statutes.[440] Such "other statutes" exemptions may require that the federal statute relied upon for exemption contain an explicit nondisclosure mandate;[441] that requirement is met by the federal law protecting SSI. Generally if the "other statutes" exemption applies, the state agency must withhold the covered information.[442]

Some states already exempt material that would constitute Federal SSI, but only if release would cause or be reasonably expected to cause actual harm.[443] To the extent that the Federal SSI provision automatically designates certain material as SSI without an actual showing of harm, application of "other statutes" exemptions allows the Federal SSI requirement to effectively amend state law.[444] Similarly, if states with expansive disclosure requirements give effect to laws in other states with less expansive disclosure requirements, a state may reduce presumption of openness under its own law.[445]

State courts have found that state public records law requirements trump "other statutes" disclosure requirements. For example, the Washington State court addressed an "other statutes" exemption in *PAWS*, *supra*. Although ultimately finding that the exemption applied on the facts in the case, the court outlined legal principles that suggested under some circumstances public records requirements would govern. The court explained that the "other statutes" exemption is an exemption to the redaction [segregation] requirement for

---

[436] *Id*. The court also held that the CIIA does not apply to submitters of PCII, so that the CIIA does not preempt requests for information made to the submitting agency under the CPRA. *Id*. at 1316–19, 385–87. *See* II.B.2, *Federal Agencies*, *supra* this report.

[437] Wisc. Newspress, Inc. v. Sch. Dist. of Sheboygan Falls, 199 Wis. 2d 768, 775–78, 546 N.W.2d 143, 146–47 (1996).

[438] Seifert v. Sch. Dist. of Sheboygan Falls, 2007 WI App 207, 740 N.W.2d 177, 187 (Ct. App. Wis. 2007).

[439] For example, the Washington statute exempts qualifying attorney work product from disclosure as an "other statute" exemption, because the attorney-client privilege statute exempts such information from disclosure. Summary of exemptions, WAC 44-14-06002, http://apps.leg.wa.gov/WAC/default.aspx?cite=44-14-06002.

[440] *Comments of the Silha Center for the Study of Media Ethics and Law on TSA Interim Final Rule on Protection of Sensitive Security Information*, July 16, 2004, TSA-2003-15569-0013, www.regulations.gov/search/Regs/home.html#documentDetail?R=0900006480313ddb (accessed Sept. 10, 2009).

[441] *E.g.*, Barry v. Wash. Post, 529 A.2d 319, 322 (1987) (exemption under federal statute must explicitly require nondisclosure); Better Gov't Ass'n v. Blagojevich, 386 Ill. App. 3d 808, 899 N.E.2d 382 (2008) (proposed disclosure must be specifically prohibited by federal or state statute or regulations in order for 5 ILL. COMP. STAT. 140/1 to apply).

[442] *E.g.,* Maryland Public Information Act, MD. CODE ANN. § 10-615, Required Denials—Other Law, www.oag.state.md.us/opengov/Appendix_C.pdf.

[443] *E.g.,* IOWA CODE § 22.7, Confidential Records. 50 [security procedures, emergency preparedness, including vulnerability assessments], http://coolice.legis.state.ia.us/CoolICE/default.asp?category=billinfo&service=IowaCode&ga=83#22.7.

[444] *See Comments of the Silha Center for the Study of Media Ethics and Law on TSA Interim Final Rule on Protection of Sensitive Security Information*, July 16, 2004, at 6, citing exemptions in ALA. CODE § 36-12-40 (1991); CONN. GEN. STAT. § 1-210(b)(19) (2003); MD. STATE GOV'T CODE ANN. § 10-613 (2003); MINN. STAT. § 13.03(1) (2003); MISS. CODE ANN. § 25-61-11 (2004); W. VA. CODE § 29B-1-4 (2003); WASH. REV. CODE § 42.17.260 (2004).

[445] [Florida] Commission on Open Government Reform, Final Report, Jan. 2009, at 102–05. Because of the potential dilution of Florida's presumption of openness, the Commission recommended against expanding the non-Florida source exemption for criminal intelligence information or criminal investigative information held by a non-Florida criminal justice agency (FLA. STAT. § 119.071(2)(b)) to include information relevant to promoting domestic security efforts. Florida Commission on Open Government Reform, Final Report, Jan. 2009, at 158–59, www.flgov.com/pdfs/og_2009finalreport.pdf.

disclosing any nonexempt portions of records. The court stated that under Washington law, the public records act incorporates those other statutes that exempt or prohibit disclosure, but only if the statutes in question "mesh" with the public records act; in the event of a conflict, the provisions of the public record act govern. Furthermore, the "other statutes" exemption only applies if the other statute explicitly identifies the exemptions in question.[446]

The Ohio Supreme Court directly addressed the question of how to resolve a conflict between the state public records requirement of disclosure and a federal privacy statute.[447] The *Enquirer* case involved a request by a newspaper for lead contamination notices issued to property owners. The court assumed for the sake of argument that the reports contained protected health information and that the Cincinnati Health Department (the withholding agency) was a covered entity under the Federal Health Insurance Portability and Accountability Act (HIPAA). Nonetheless, the court concluded that the federal statute did not supersede state disclosure requirements because the state public records disclosure mandate met the "required by law" exception to HIPAA's nondisclosure requirements.

Where the effect of an "other statutes" provision is to prohibit the disclosure of information that would otherwise be disclosed under state law, such provisions do not necessarily eliminate the need to follow the procedural requirements of the state public records law. For example, the Virginia Supreme Court addressed the question of whether federal airport security laws and regulations preempted the requirements of the Virginia FOIA in *Fenter v. Norfolk Airport Authority*.[448]

In *Fenter,* the plaintiff had asked the Norfolk Airport Authority for a copy of any federal or Virginia statute or regulation that authorized vehicle searches at the airport.[449] The plaintiff made an initial request on March 8, 2006; within several days the authority notified the plaintiff that his request had been forwarded to counsel for response. On March 21, 2006, plaintiff made a second request for "the history or circumstances relating to the erection of" the airport search signs; the Authority's counsel responded within a week advising plaintiff that the authority had contacted TSA and would get back to him when it had heard from TSA. On May 6, 2006, plaintiff requested copies of any records of the correspondence between the authority and TSA regarding the signs and plaintiff's requests for information; within 2 days the authority's executive director responded that all further requests should be directed to counsel, who was copied on the response. Having received no further response and having been advised by the Virginia FOIA Advisory Council that the authority had not met Virginia FOIA's procedural requirements, plaintiff filed a complaint on July 25, 2006.

The *Fenter* court reviewed the applicable state requirements concerning general availability of records, the requirement to narrowly construe exemptions, the public body's burden of proof on exemptions, and the procedural requirements under Virginia's FOIA.[450] The court found that the authority's immediate responses to the plaintiff's second and third requests for information did not meet the Virginia FOIA's procedural requirements. Moreover, once plaintiff filed suit, the authority eventually produced nonsensitive, nonexempt material related to the second and third requests for information. The court rejected the authority's preemption argument and agreed with the plaintiff that federal law and regulations did not preempt the procedural requirements of state law or the need to produce documents that were not SSI. Furthermore, the court found

[446] Progressive Animal Welfare Society, 125 Wash. 2d 243.

[447] State *ex rel*. Enquirer v. Daniels, 108 Ohio St. 3d 518, 2006 Ohio 1215, 844 N.E.2d 1181 (2006).

[448] 274 Va. 524, 649 S.E.2d 704 (Va. 2007).

[449] The specific request was:

> There are signs on the access roads to the Norfolk International Airport stating that "All vehicles entering airport are subject to search." Please provide me a copy of any Federal or Virginia statute or regulation authorizing the Airport Authority to search any vehicle on airport property, outside the Federal "sterile area," without prior probable cause or a valid search warrant issued by a Federal or Virginia court.

Id. at 706.

[450] *Id*. at 707–708. At the time the complaint was filed the Virginia Freedom of Information Act, Code § 2.2-3704(B) provided:

> Any public body that is subject to [the Act] and that is the custodian of the requested records shall promptly, but in all cases within five working days of receiving a request, make one of the following responses:
>
> 1. The requested records will be provided to the requester.
>
> 2. The requested records will be entirely withheld because their release is prohibited by law or the custodian has exercised his discretion to withhold the records in accordance with [the Act]. Such response shall (i) be in writing, (ii) identify with reasonable particularity the volume and subject matter of withheld records, and (iii) cite, as to each category of withheld records, the specific Code section that authorizes the withholding of the records.
>
> 3. The requested records will be provided in part and withheld in part because the release of part of the records is prohibited by law or the custodian has exercised his discretion to withhold a portion of the records in accordance with [the Act]. Such response shall (i) be in writing, (ii) identify with reasonable particularity the subject matter of withheld portions, and (iii) cite, as to each category of withheld records, the specific Code section that authorizes the withholding of the records. When a portion of a requested record is withheld, the public body may delete or excise only that portion of the record to which an exemption applies and shall release the remainder of the record.
>
> 4. It is not practically possible to provide the requested records or to determine whether they are available within the five-work-day period. Such response shall be in writing and specify the conditions that make a response impossible. If the response is made within five working days, the public body shall have an additional seven work days in which to provide one of the three preceding responses.

The court noted that the subsequent amendment of this provision did not make substantive changes. *Id.* at 708.

the plaintiff entitled to reasonable costs and attorney fees.[451]

3. Trade Secrets/Commercial Information

Exemptions for trade secrets/commercial information should already be familiar to transit agencies. Some of the recommended procedures for this exemption may also apply—directly or with some modification—to security information, either that provided by the transit agency to bidders and contractors during the procurement process or information developed by bidders and contractors. For example, FTA's *Best Practices Procurement Manual* discusses the potential conflict between a vendor's trade secret interest and the transit agency's obligations under state sunshine laws. FTA suggests four best practices to resolve this conflict: returning the confidential data once the procurement is completed; inspecting the data off site; allowing a third party to evaluate the data (although an agent of the public agency may also be subject to public records requirements); and using contract provisions that grant/require the trade secret holder to defend the agency against actions seeking public disclosure.[452]

State law may address directly limitations on disclosure of proprietary information during the bidding process.[453]

4. Inter-Agency/Intra-Agency Memoranda[454]

Security information contained in inter-agency or intra-agency memoranda may be exempt from disclosure, generally under the deliberative process privilege. This protection is more likely to extend to records relating to contract deliberations than to contract documents themselves. The typical limitations of this privilege are illustrated in the Washington Supreme Court's discussion in the *PAWS* case, *supra*. The court noted that the deliberative process exemption under the Washington public records act does not apply to all documents in which opinions are expressed, but only those documents in which the opinions relate to policy formulation and the disclosure of which would expose the deliberative process, as opposed to exposing the facts on which the deliberation is based. The court set forth this standard:

> In order to rely on this exemption, an agency must show that the records contain predecisional opinions or recommendations of subordinates expressed as part of a deliberative process; that disclosure would be injurious to the deliberative or consultative function of the process; that disclosure would inhibit the flow of recommendations, observations, and opinions; and finally, that the materials covered by the exemption reflect policy recommendations and opinions and not the raw factual data on which a decision is based.[455]

In addition, under Washington State law, once the policies or recommendations are implemented, the information is no longer protected. The exemption is not limited to intra-agency documents prepared by a government agency. For example, in addition to applying this exemption in *PAWS* to documents prepared by nongovernmental scientists, a Washington appellate court held the exemption covered negotiation notes of members of a police union.[456]

D. Records Management Laws

Often the purview of the Secretary of State,[457] records management requirements may also be administered by a public records commission,[458] a local records board,[459] the state library/archives,[460] or some other entity. These agencies often offer guidance for local agencies concerning record retention and record destruction requirements.[461] State law is likely to cover public transit agencies. Such laws may cover contract agencies as well.[462]

The length of time that local agencies are required to maintain bid documents may vary from as short a period as 2 years to as long as 10 years, depending in part

---

[451] *Id.* at 709.

[452] *See, e.g.,* BPPM, 8.2.4.1 Disclosure of Trade Secrets, at 32–33.

[453] Nevada: NEV. REV. STAT. 332.061, Limitation on disclosure of proprietary information and of bid containing provision requiring negotiation or evaluation. [Chapter 32: Local Government Purchasing]; NEV. REV. STAT. 332.025, Other terms defined, [Includes definition of proprietary information] www.leg.state.nv.us/NRS/NRS-332.html#NRS332Sec025.

[454] *E.g.*, MD. CODE, § 10-618(b), Permissible denials: *Inter-agency and intra-agency documents*.

[455] Progressive Animal Welfare Society, 125 Wash. 2d 256.

[456] Am. Civil Liberties Union of Wash. v. City of Seattle, 121 Wash. App. 544, 89 P.3d 295 (Wash. App. Div. 1 2004).

[457] *E.g.*, Washington State, www.secstate.wa.gov/archives/RecordsManagement/.

[458] *E.g.*, New Mexico Commission of Public Records, www.nmcpr.state.nm.us/commiss/commission_hm.htm. *See* N.M. STAT. ANN. ch. 14, art. 3, Public Records, www.conwaygreene.com/nmsu/lpext.dll?f=templates&fn=main-h.htm&2.0.

[459] *E.g.*, The Missouri Secretary of State appoints a local records board charged with developing record retention schedules for local governments and agencies. MO. REV. STAT. § 109.255, www.moga.mo.gov/statutes/C100-199/1090000255.HTM. Heads of local agencies are then charged with submitting proposed schedules, consistent with the local records board standards, for various types of records under their control. MO. REV. STAT. § 109.241, www.moga.mo.gov/statutes/C100-199/1090000241.HTM.

[460] Texas State Library and Archives Commission, Preservation and Management of State Records and Other Historical Resources Government Code, ch. 441, subch. L, www.tsl.state.tx.us/slrm/recordspubs/stbull04.html#pres.

[461] *E.g.*, Alabama: Government Records Division, Department of Archives and History, offers records management assistance to local officials, www.archives.state.al.us/officials/rec-center.html; Florida: State Library and Archives offers services for records managers, http://dlis.dos.state.fl.us/index_RecordsManagers.cfm.

[462] *See, e.g.*, Circular Letter 97-07-SCA: Administration of Public Records of Privatized County and Local Functions and Services, www.state.nj.us/infobank/circular/cir9707c.htm.

on the type of contract and whether or not the bid was successful.[463] For example, Connecticut requires that local government agency bid documents for public works construction projects (whether accepted or not) be retained for 6 years after project completion or 6 years after filing if the project is not built, and then destroyed; bid documents for public works service/supply projects (whether accepted or not) be retained for 3 years after the audit and then destroyed; and construction documents be retained for the life of the structure.[464] State statutes may specifically cover retention of state DOT records.[465] Record retention guidance may specify how documents are to be disposed of after the required retention period. Montana, for example, specifies that contract protest records are to be shredded 4 years after the protests are resolved.[466] Federal requirements for disposal of SSI should be followed if they are more stringent than state record disposal requirements.

The increasing use of electronic storage of information presents special challenges, as it is not always as clear what electronically stored information constitutes public records as it is for information on paper.

IV. TRANSIT AGENCY PRACTICES

A thorough understanding of requirements for handling security information is needed both to ensure that procurement personnel treat such information appropriately and that they include appropriate safeguards in bidding and contract requirements. Developing effective procedures is a critical element; ensuring appropriate implementation is perhaps both more critical and more difficult.[467]

This section discusses actual transportation agency practices concerning protection of security information. The discussion is based on both agency responses to questions posed by the author and secondary research. The intent of this section is to allow transit agencies to consider approaches adopted by other agencies as they formulate their own policies. Given the sensitivity of the topic, this section uses anonymous titles for transit agencies that provided responses directly to the author.

A. Transit Agency A[468]

Agency A is a bus-only transit system located in Northern California. The agency operates 15 weekday local bus routes and 3 weekend/holiday local bus routes, as well as commuter routes, serving a population of almost 250,000. Agency A addresses SSI under the agency's safety and security plan. The agency has established an internal audit system of its SSI control procedures.

The safety and security plan treats SSI consistent with the guidance in FTA's *Sensitive Security Information (SSI) Designation, Markings, and Control* document. Previously the agency relied on the Recommended Practices from the American Public Transportation Association's Emergency Management Program Standards. The agency does not protect information other than SSI from disclosure based on security grounds.

The agency's SSI practices were formulated by the chief executive officer, chief operating officer, and director of administrative services. The SSI practices do not directly address procurement. However, the chief operating officer and the agency's procurement officer discuss SSI requirements, if applicable, when they develop procurement documents. This analysis is limited to security-related bid and contract documents. The practice is to exclude SSI from procurement documents to the extent feasible, limiting inclusion of SSI in contract specifications to the bare essentials required to allow a meaningful response to the solicitation.

Agency A has had a very low volume of security projects and thus has had limited experience in deploying its SSI practices. To the extent necessary, the agency would deploy one or more of the following methods for controlling contractor access to SSI in the procurement process, depending on how detrimental to transportation safety it would be to allow the information in question to be made public:

- Performing background checks.
- Charging a fee to receive the documents.
- Restricting review of contract documents to the requestor.
- Requiring the requestor to sign a nondisclosure form.

[463] *See*, *e.g.*, N.M. CODE, 1.19.8.109, Capital Project Files [Fiscal or contractual documents (bids, quotes, agreements, contracts, etc.): 10 years after completion of project; Technical documents (e.g. blueprints, architectural drawings, soil tests or analyses, engineering specifications, etc.): permanent; All other documents: 2 years after close of fiscal year in which project completed], www.nmcpr.state.nm.us/nmac/parts/title01/01.019.0008.htm; Washington State Archives, Office of the Secretary of State, *Local Government Common Records Retention Schedule (CORE) Version 1.0* (December 2008), 1.4 contracts/agreements, www.secstate.wa.gov/_assets/archives/RecordsManagement/CORE10.pdf.

[464] Office of the Public Records Administrator (Connecticut State Library), Municipal Records Retention Schedule M9, Public Works, www.cslib.org/publicrecords/retpbworks.pdf.

[465] *E.g.*, Nevada, NEV. REV. STAT. 239.085 State records: Disposition by Department of Transportation, www.leg.state.nv.us/NRS/NRS-239.html#NRS239Sec073.

[466] Montana record retention schedule for purchasing procurements: http://sos.mt.gov/Records/forms/state/State_Schedule4.pdf.

[467] *See* Office of the New York State Comptroller, Metropolitan Transportation Authority: Controls Over Security-Sensitive Information for the Capital Projects Program, Report 2006-S-6, www.osc.state.ny.us/audits/allaudits/093006/06s6.pdf.

[468] The description of Agency A's security/procurement practices is based on responses from the agency to questions posed by the author. Responses are maintained in the author's files.

The agency also limits which procurement personnel have access to SSI.

Agency A provides SSI training to all employees; the subject covered depends on the job category in question.

B. Los Angeles County Metropolitan Transportation Authority[469]

The Los Angeles County Metropolitan Transportation Authority (MTA) has a written records management policy (RMP) to ensure compliance with the California Public Records Act, as well as the agency's statutory obligations concerning records disposition. The RMP covers creation, indexing, production, retention, protection, security and disposition of agency records. Covered records include correspondence, memoranda, reports, maps, tapes, photographic films/prints, charts, drawings, computer-generated and -maintained records, machine-readable records, and phonographic records. Email is covered as well. The MTA's Records Management Center (RMC) is responsible for administering the RMP, including providing training, while department heads are responsible for program compliance within their departments. Each department appoints a records coordinator to work with the RMC, managing department records pursuant to RMC guidelines.

The RMC develops the agency's records retention schedule, which identifies categories of security-sensitive documents. Any changes to the schedule are reviewed by the agency's legal counsel. RMC periodically inventories department records to ensure compliance with the retention schedule. RMC oversees records inactivation, inactive records retrieval, and records destruction pursuant to the retention schedule. Sensitive security information is shredded, pulped, erased by permanent means, or otherwise made illegible and unusable.

The RMP protocol for active file management requires maintaining security-sensitive documents such as facility as-built drawings in secure locations separated from documents that are not confidential or security sensitive, with access limited to designated staff. Each department is required to keep a list of designated personnel, along with their approved access levels. RMP protocol also requires purging drafts, duplicates, and nonsignificant working papers from active files on a regular basis. Sensitive security documents are required to be marked as such within the agency's document management system.

Only the RMC and legal counsel have the authority to determine which records are available to the public. All agency employees receive training to this effect, including being put on notice that they are to consult with RMC and legal counsel concerning any third party requests for MTA documents.

The RMP contains a section on exempt security-sensitive and privileged documents. The policy notes that due to attacks, attempted attacks, and threats against facilities, MTA limits access to categories of records that previously may have been publicly available. The intent of treatment of such documents under the policy is to ensure that access will be limited to individuals with an actual need to know or work with the records. Section 2.1 of the RMP lists types of documents to be considered security sensitive and specifies the need for separate maintenance in a secure environment of such documents.[470] The RMP lists the following record categories as coming under the sensitive security classification: construction records (design documents, final as-built drawings required by contract); engineering documents (detailed specifications, including geotechnical information); systems documents (describing how safety- and security-related systems operate); operations records (detailing movements to and from service route); facility information (security and fueling system information); vehicle design documents; and security records (documents describing MTA security responses).

C. Agency C[471]

Agency C is the organization responsible for capital construction projects for a large multimodal transportation authority. Agency C works with sister agencies of the transportation authority.

Agency C has an SSI handbook covering the following elements: procedures for handling Agency C's SSI; roles and responsibilities of Agency C and vendor personnel; Agency C evaluation guide to identify types of information to be protected; information technology; company nondisclosure and confidentiality agreements;

[469] The description of LACMTA's records management practices is based on a review of the agency's Records Management Policy. The records management services can be reviewed at http://www.metro.net/about/library/records-services/records-management/records-services/.

[470] Section 2.1, Identifying Security Sensitive and Privileged Records, specifically provides:

> RMC, along with each department shall identify security sensitive documents that shall include, but not be limited to, the construction of all MTA facilities; operation of light and heavy rail systems; communication, power, control and emergency backup systems, emergency access. Ingress and egress methods and plans; bus scheduling process; personnel deployment plans; security plans and interagency emergency or security communications; individual and computer system access codes and methods; software; and other similarly related items.
>
> Any document considered security sensitive shall be maintained in a separate protected environment and may be retained with confidential records by RMC. The manner of protecting such documents shall be dictated by the form and condition of the particular record. Once a document is identified as security sensitive, access to it shall be immediately limited, and as appropriate, moved to a secure location. The document may be copied to a protected environment to protect the information or to limit its availability to those persons authorized to access the information.

[471] The description of Agency C's security/procurement practices is based on a review of the company's Security Sensitive Information Handbook, which identifies procedures to be used during implementation of Agency C security projects.

Agency C nondisclosure and confidentiality agreements for individuals; employee employment and resume verification; and procurement procedures.

Personnel involved in Agency C's SSI process includes the Agency C security officer, who is responsible for implementing and overseeing SSI procedures and key in deciding what information is protected; the agency security officer, who is the SSI point person for the sister agency, assisting the Agency C security officer in implementing required briefings and training; and the Agency C/agency project manager, who is authorized to handle SSI. The security officers must be U.S. citizens or permanent residents. Both the project manager and all Agency C/agency employees involved in supervising consultants, contractors, and subcontractors of projects related to Agency C SSI are required to sign NDAs and undergo employment and resume verification, as are all vendor project managers, principals of vendor companies, and vendor employees working on design and construction of projects related to Agency C SSI.

Agency C requires consultants and contractors to provide training to all of their employees authorized to access Agency C SSI, with disclosure of SSI only authorized as needed to perform official duties and on a need-to-know basis. Agency C receives a list of authorized vendor employees. Vendors must have a document control system to track the location and number of copies of documents containing Agency C SSI. Vendors must also develop an Information Technology System Management Plan covering physical, operational, and personnel procedures; Agency C must approve the plan and employees must undergo information technology security awareness training.

Agency C policy ties these vendor security requirements to the procurement process by mandating that they be made a material condition of contracts that require access to Agency C SSI, with the contracts subject to termination for default where willful misconduct or lack of good faith leads to noncompliance. Vendors are also required to include these provisions in all subcontracts. Once a contract containing SSI is completed, the vendor must return all originals to Agency C and destroy all copies, following procedures set forth in the handbook.

Measures to safeguard SSI include:

- Prohibiting discussion of SSI in public conveyances or places, via wireless phone or radio; limiting use of discussion via speakerphone to closed-door locations.
- Storing SSI with password protection or in secure containers with no indication that containers store SSI; maintaining list of individuals with access to each container.
- Removing SSI from information technology system when no longer required to be on system.
- Maintaining physical security to prevent unauthorized access to hardware and software related to SSI, e.g., by requiring User IDs and keeping unattended information technology systems in locked space.
- Using a firewall security system for SSI information technology storage systems.
- Encrypting SSI data transfer.
- Requiring security training for personnel with access to SSI information technology systems.
- Centralizing physical storage of SSI as much as practicable.
- Prohibiting removal of SSI from work area without Agency C authorization.
- Once projects are complete, using card readers to track access to storage locations.
- Establishing system to ensure reproduction of SSI is held to a minimum and accomplished by authorized employees; marking copies as originals are marked.
- Destroying SSI to prevent unauthorized retrieval; logging destroyed documents through document control system (date of disposal, identification of material destroyed, signature of individuals designated to destroy and witness destruction).
- Transmitting SSI in a manner preventing loss or unauthorized access: receipt required; no marking on package to indicate inclusion of SSI; packages to be returned if authorized recipients not present and not to be left unattended.
- Limiting access to need to know: necessary for recipient's job performance, recipient has read and understands agency SSI procedures, and has signed NDA.

Additional security measures include requiring all SSI documents to be marked as specified in the handbook; maintaining lists of authorized internal and external SSI recipients, with individuals removed from the authorized list when their need to know expires; and maintaining a list of all individuals who have or have had access, for investigative purposes; maintaining a document control system with log information as specified in the handbook.

Agency C's audit program evaluates consultant and vendor compliance with the security requirements set forth in the handbook.

Project managers are responsible for developing project-specific evaluation guides based on the agency's generic evaluation guide and for identifying information that must be treated as SSI pursuant to the project-specific evaluation guide. If a vendor employee believes information not designated as SSI may or should be SSI, the individual should request an evaluation by the project manager and protect the information accordingly until a decision is made. SSI that has been made public should still be protected until the Agency C security officer makes a formal decision.

Agency C's NDA covers the scope of SSI, obligations of nondisclosure, requirements for protection of information (including notifying Agency C of any subpoenas for SSI), and return of information. Potential recipients of SSI are given a copy of the SSI handbook and are required to execute and affidavit acknowledging receipt of the handbook.

The handbook recommends that Agency C only release bid documents containing SSI to bidders that have

completed NDAs and Information and Responsibility Request forms covering security questions.

D. Transit Agency D[472]

Agency D is a large multimodal transit agency. As of October 2009, Agency D was in the process of developing its own SSI policy. Departments involved in the development process include capital programs, capital program management, legal, procurement, and engineering. The policy will cover procurement as well as other issues.

Agency D does protect information other than SSI from disclosure based on security grounds, and controls access to all information pertaining to construction projects. To date the agency has only had occasion to review security-related projects for CII/SSI. However, as it develops its SSI policy, Agency D intends to require the review of all projects to determine the need for controlling access to procurement documents based on the nature of the project. Rather than focusing on whether the project provides security, the policy will focus on whether information in the procurement is sensitive. For example, a procurement for a project to place cameras in a visible manner in a public area may not require restricted access to procurement information, while a procurement to do structural work on a subway tunnel may require restricted access because of the need to review sensitive structural information to bid and to carry out the contract. This approach allows for the prioritization of security information by the incremental damage a threat source would gain by knowing the information.

Agency D controls contractor access to SSI and other security information by requiring prospective vendors to register with FedBizOpps,[473] the federal contracting Web site database. Registration on this Web site requires getting cleared to receive sensitive material. Agency D is also considering carrying out some security-related construction work in-house, which would avoid the need to manage contractor access to security information.

Agency D does have a single point of contact in each of its major groups for handling SSI. Procedurally, project design managers review project information for SSI and notify procurement of the SSI classification. This requires both engineers and procurement personnel to be trained on SSI classification and management.

E. Agency E[474]

Agency E is a transportation authority responsible for surface transportation in a county in the western United States. Agency E administers the county's bus and paratransit public transportation system.

Agency E requires all employees working on vulnerability assessments, security plans, and security enhancement plans to execute confidentiality agreements specifically regarding requirements for maintaining confidentiality of material and acknowledging penalties for noncompliance. Agency E's Security/Safety Section reviews only security-related bids for CII/SSI.

F. Virginia Department of Transportation[475]

The Virginia Department of Transportation's (VDOT) Critical Infrastructure Information/Sensitive Security Information (CII/SSI) Policy is an internal document. However, elements of the policy are described in publicly available documents, such as VDOT's guide to identifying CII/SSI. In addition, VDOT's CII/SSI Guide for Vendors and Contractors is publicly available.

The guide cautions that if the information is customarily public knowledge or the general public has a need to know the information, then it is not CII/SSI. The guide is based on the criteria on the safety and security exemptions in the Virginia Freedom of Information Act, which provides that records falling under the exemptions are excluded from the mandatory disclosure provisions of the act, but may be disclosed at the custodian's discretion unless otherwise required by law.

The guide lists categories of information that might be CII/SSI. These include:

- Engineering and construction drawings and plans that would reveal critical structural components or security equipment and systems, if disclosure would jeopardize the health or safety of any person or structure.
- Documentation describing the design, function, operation or access control features of any security system, manual or automated, used to control access to or use of any automated data processing or telecommunications system.
- Plans and information to prevent or respond to terrorist activity, if disclosure would jeopardize the safety of any person, including vulnerability assess-

[472] The description of Agency D's security/procurement practices is based on responses from the agency to questions posed by the author. Responses are maintained in the author's files.

[473] www.fbo.gov/.

[474] The description of Agency E's security/procurement practices is based on responses from the agency to questions posed by the author. Responses are maintained in the author's files.

[475] The description of VDOT's sensitive information protection procedures is based on a review of several publicly available documents: Location and Design Division's Instructional and Informational Memorandum on Procedures for Protecting Sensitive Information, www.extranet.vdot.state.va.us/locdes/electronic%20pubs/Bridge%20Manuals/IIM/SBIIM71.pdf (accessed Apr. 1, 2009); VDOT's CII/SSI Guide for Vendors and Contractors, http://www.virginiadot.org/business/resources/const/CII_SSIGuideV6.0InterimRevisionFINAL.PDF; VDOT's Critical Infrastructure Information (CII) Sensitive Security Information (SSI) Agreement to Establish a Company Representative, http://vdotforms.vdot.virginia.gov/SearchResults.aspx?filename=CII%20Company%20Rep%20V5.pdf (accessed Apr. 1, 2009); VDOT's Guide to identifying CII/SSI, http://vdotforms.vdot.virginia.gov/SearchResults.aspx?filename=Guide%20to%20Identifying%20CII%20SSI.pdf.

ments or operational, procedural, transportation, and tactical planning or training manuals.

- Information revealing surveillance techniques, personnel deployments, or operational and transportation plans and protocols.
- Information concerning threats against transportation.

For reviewing records that fall into the categories that might be CII/SSI, the guide recommends considering these factors about the need to protect CII/SSI:

- What impact could the information have if it were inadvertently transferred to an unintended audience?
- Does the information provide details concerning security procedures and capabilities?
- Could someone use the information to target personnel, facilities, or operations?
- How could someone intent on causing harm misuse the information?
- Could the use of this information be dangerous if it were combined with other publicly available information?

The policy requires custodians to take reasonable steps to minimize unauthorized access to CII/SSI during working hours and to secure it after working hours in a locked desk or file cabinet or similar secure container. Each person who works with CII/SSI is personally responsible for safeguarding it. Information containing CII/SSI should only be released to persons with a legitimate VDOT-related need to know and who have signed VDOT's NDAs. It is uncertain whether the policy itself sets forth steps for establishing the need to know.

VDOT requires contractors to sign individual NDAs before gaining access to VDOT CII/SSI. In addition, a company representative is required to sign a company agreement accepting responsibility on behalf of the company for the actions of all company employees in regard to VDOT CII/SSI in the company's custody or control, acknowledging that all individuals involved with the project in question who will have access to VDOT CII/SSI must sign an NDA before receiving such access; and acknowledging the need-to-know nature of the CII/SSI and penalties for failing to protect the information. The agreement includes a list of responsibilities in handling CII/SSI, including protection, use and storage, reproduction, disposal, and transmission.

V. APPLYING SECURITY AND CONTRACT MANAGEMENT REQUIREMENTS TO THE COMPETITIVE PROCUREMENT PROCESS

The federal and state legal requirements discussed above clearly have an effect on how procurement personnel manage contract documents containing security information, including how those personnel respond to requests for information under state public records laws. For example, infrastructure information submitted to DHS or USDOT may become protected from disclosure by those agencies. However, it is an evolving question whether submitting such information to covered federal agencies renders the information protected from disclosure by the local agency that submits it. At least one state court has distinguished between the obligation of the federal agency receiving protected CII to maintain confidentiality and that of the local agency submitting information otherwise disclosable under state law to keep such information confidential merely because it was submitted to a federal agency.

In addition, transit agencies must distinguish between the obligation to control documents containing SSI and the obligation to disclose non-SSI information in such documents. For purposes of control, if a document contains SSI, the entire document must be secured while in agency control. For purposes of public records requests, if a disclosure request is made for a document containing SSI, many state laws require the agency to redact the SSI and release the unredacted portion of the document, if reasonably feasible.

Finally, transit agencies should be aware of the legal distinctions between SSI and restricted security information (information that is not SSI but has been identified as potentially harmful to security if disclosed), as SSI is protected under federal law but restricted security information is not.

Moreover, the sometime conflicting public policy purposes of the various requirements demand that procurement personnel balance those purposes as they develop and manage procurement documents. This section highlights several areas where that effect comes into play. These include measures that may minimize the need to balance competing needs for security and disclosure; decisions on when security information should be disclosed; and procedures for maintaining contract records containing security information.

A. Minimizing Need to Balance Security and Transparency[476]

Good contract management procedures applied to management of SSI and restricted security information, just as applied to the handling of trade secrets and confidential financial information, will help balance the public right to know and need to know. On the other hand, poor recordkeeping, such as lacking a contract administration system or having no written record of procurement history,[477] may create problems in properly

[476] The Florida Attorney General has provided a good analysis of the balancing issue and factors to consider in determining whether to disclose SSI in competitive bidding. Florida Attorney General Advisory Legal Opinion AGO 2002-74—Nov. 4, 2002, http://myfloridalegal.com/ago.nsf/Opinions/D4CFF22D8B492BDF85256C6700541A22 (accessed Apr. 1, 2009); Summary: http://brechner.org/reports/2002/12dec2002.pdf (accessed Apr. 1, 2009).

[477] U.S. GOV'T ACCOUNTABILITY OFFICE, PUBLIC TRANSPORTATION: FTA'S TRIENNIAL REVIEW PROGRAM HAS IMPROVED, BUT ASSESSMENTS OF GRANTEES' PERFORMANCE COULD BE ENHANCED 15 (2009) (citing deficiency codes in Triennial Reviews), www.gao.gov/new.items/d09603.pdf.

managing this information. In addition, state law may require that public records be designed to facilitate segregation to the extent practicable. Such requirements may support an approach of not scattering security information throughout the documentation (assuming security information cannot be kept out of procurement documentation altogether).

The drafting of bid specifications and other contract documents is a very good place to apply the "need to know" concept by asking: Is there a compelling need to include SSI/Restricted Security Information in the documents? For example, if bid documents related to a security project themselves only specify security parameters—which are disclosable—as opposed to detailed operations requirements, [478] those bid documents can be made available for the same public inspection as bid documents that have no relation to security. This approach requires making any SSI/restricted security information needed for bid response available to bidders separately, presumably under properly controlled circumstances. However, the practicability of keeping such information entirely out of contract documents will vary, largely depending on the particular procurement at issue, and to some extent on the tracking capabilities of the agency's procurement process. Alternatively, SSI may be included in an appendix, which can be redacted from public records requests.[479]

It is important that the personnel structuring procurement documents understand these security issues. The authors of the *Security and Emergency Preparedness Planning Guide*, *supra*, recommend that the agency security manager have authority in overseeing security issues in the procurement process.[480]

B. Deciding Whether Information Should Be Disclosed

Information that has been classified as SSI should not be disclosed to the public under state public records acts. However, circumstances may change over time so that information originally classified as SSI may no longer merit that classification when a particular request is made. Restricted security information may or may not be exempt from disclosure, depending on state law. When a transit agency official considers a request for information in either category, the deciding official must consider whether 1) the requested information is covered by an exemption from disclosure requirements; 2) if covered, the official has the discretion to disclose the information; and 3) if the discretion exists, whether it should be exercised. In the case of information covered solely by state law, this will depend on whether applicable exemptions are mandatory or permissive.[481] The question of how to release such information to persons with a need to know, subject to limitations, is discussed below under V.C, Procedures for Maintaining Contract Records Containing CII/SSI/Restricted Security Information.

1. Determining When Disclosure Threatens Public Security[482]

The very existence of security measures is often public, while the operational details of the measures are not.[483] For example, if a transit agency purchases closed circuit security cameras for buses, the existence of those cameras is likely to be readily apparent. If so, disclosing information about a contract to purchase readily discernible security cameras is not likely to threaten public security. On the other hand, details of enhancements to those cameras, not readily apparent from observing the cameras in place, may not be publicly announced. Disclosing information about commercially available security systems, commercially available system effectiveness data, and accepted construction techniques is not likely to threaten public security, while disclosing unique information about methods to defeat those security systems could assist persons seeking to attack the systems. Even information identifying critical system elements is not likely to threaten public security if the equipment is readily observable to the public.

The distinction between existence/parameters (disclosable) and details of execution (sensitive) is critical in classifying information. For example, the release of generic security criteria is not likely to threaten public security, while releasing site-specific information generated from such criteria could be harmful. Similarly, releasing information about the general location of security projects is not likely to result in harm, while revealing explicit details or capabilities could threaten public security. This is analogous to notice requirements in the Fourth Amendment context, where requirements for conducting random searches must be disclosed, but not the manner in which the government will attempt to ensure that search requirements are not violated.[484]

State requirements for disclosing the results of bridge inspections illustrate the possible differences in

[478] *E.g.*, Blank TSA vulnerability checklist is considered disclosable. It does not become SSI until it has been completed with specific information.

[479] CHANDLER, SUTHERLAND, & ELDREDGE, *supra* note 164, at 5.

[480] BALOG, BOYD, & CATON, *supra* note 1, at 25–26 (2003), http://transit-safety.volpe.dot.gov/publications/security/PlanningGuide.pdf.

[481] Maryland, for example, has both mandatory and discretionary exemptions, www.oag.state.md.us/Opengov/ChapterIII.pdf.

[482] TRANSTECH MANAGEMENT, INC., *supra* note 1, at 3–4.

[483] *E.g.*, New Jersey purchase of buses with closed-circuit camera systems, enhancing Newark Penn Station: Jan. 23, 2007, Minutes of NJ Transit Board of Directors meeting, at 6, www.njtransit.com/pdf/Jan%2023%202007.pdf (accessed Feb. 28, 2009); Michael Fickes, *Preventing Mass Transit Terror Attacks*, GOVERNMENT SECURITY MAGAZINE, Oct. 1, 2005 (describing security measures taken by NYMTA), http://govtsecurity.com/transportation_security/preventing_mass_transit/ (accessed Feb. 28, 2009).

[484] *See*, *e.g.*, WAITE, *supra* note 10, at 23.

approaches to disclosure. Some states have taken the position that detailed bridge inspection reports would provide information to would-be terrorists concerning structural weaknesses; these states deny full access to such reports. Other states make such reports available to the public, although in some cases only at state offices.[485]

A number of reports and guidance documents suggest questions to ask in determining how to classify information and whether to release particular information.[486] These questions, which should be considered in relation to each other, include:

- Can the information be used to select a target for terrorist attack?[487]
- Does the information make its subject a more attractive target or increase the risk of attack?
- Does the public need to know the information? If so, can the information that the public needs to know be separated from information that could increase the threat to system security?
- Is the same or similar information readily available from other sources, including first-hand observation of public areas or via the Internet?
- How does the agency normally treat this type of information? Are the number of copies and location of copies tracked?
- What is the agency's threat environment?

2. Permissibility of Distinguishing Based on Requester's Identity

The requester's identity could potentially enter into the assessment of the potential threat of releasing the information. Factors to consider include:

- Some states require employees to report suspicious or unusual requests for information to legal counsel or other specified authorities on records management.[488] The viability of this approach under a specific state law may depend on how the determination is made that a request is unusual or suspicious.
- Denying requests based on the requester's identity or the purpose of the request may be illegal under state law, although some states do require identification before disclosure.[489] Transit agencies are advised to analyze whether flagging requests for certain types of information for special review is consistent with state law, particularly if state law prohibits denying requests based on the requester's identity.

C. Procedures for Maintaining Contract Records Containing CII/SSI/Restricted Security Information[490]

The length of time that a transit agency must comply with record disclosure and management requirements will be governed by federal, state, and local record retention requirements, so obviously it is important to be aware of those requirements. The length of time that a record containing security information must be managed in a controlled fashion could affect the decision to include such information in procurement documentation.

There are important legal distinctions between managing federally-designated CII/SSI and managing restricted security information. Federal law imposes specific requirements for protecting CII/SSI, along with liability for unauthorized disclosure. In addition, being classified as CII will arguably limit the agency's use of the information so classified. A transit agency may, as a matter of policy, apply the same restrictions on disclosure to restricted security information as those required by law for CII/SSI. However, there should be no state statutory penalty for unauthorized disclosure of restricted security information unless state law prohibits the disclosure of the particular information at issue, in which case unauthorized disclosure would violate the state law containing the prohibition, with whatever penalty that law provides.

While not required for transit agencies, GAO recommendations for improving administration of SSI and congressional requirements for TSA set forth some principles to consider in managing SSI to ensure compliance with federal law and regulations. Steps recommended by GAO include establishing guidance and procedures for using TSA regulations to determine what constitutes SSI, including offering examples of SSI; establishing responsibility for the identification and designation of SSI; creating and promulgating policies and procedures within TSA for providing training to those making SSI determinations; establishing internal controls that define responsibilities for monitoring compli-

[485] Jeff Martin, *Some States Close Bridge Inspection Data to Public*, USA TODAY, July 24, 2008, www.usatoday.com/news/nation/2008-07-24-bridgereports_N.htm (accessed Feb. 28, 2009).

[486] *E.g.,* TRANSTECH MANAGEMENT, INC., *supra* note 1, at 7–8; VDOT's CII/SSI Guide for Vendors and Contractors, http://www.virginiadot.org/business/resources/const/CII_SSIGuideV6.0InterimRevisionFINAL.PDF.

[487] For an example of information deemed disclosable, see the drawing included in a Port Authority of New York and New Jersey prequalification document. www.panynj.info/DoingBusinessWith/contractors/pdfs/RFQDOC_WTC224545.pdf.

[488] TRANSTECH MANAGEMENT, INC., *supra* note 1, at 7.

[489] Nevada imposes restrictions on persons who may inspect specified classes of documents that the governor has determined are likely to "create a substantial likelihood of compromising, jeopardizing or otherwise threatening the public health, safety or welfare" if released. NEV. REV. STAT. 239C.210, Confidentiality of certain documents, records, or other items of information upon declaration of Governor; penalties; NEV. REV. STAT. 239C.220, Inspection of restricted documents, www.leg.state.nv.us/NRS/NRS-239C.html.

[490] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 138, at 4.

ance with SSI regulations, policies, and procedures; and communicating these responsibilities throughout TSA.[491] As noted, *supra*, Congress specifically required TSA to revise its management directive to review requests to publicly release SSI in a timely manner, including SSI that is at least 3 years old. GAO has also recommended that the Office of Management and Budget work to develop a government-wide directive that provides guidance on how to control sensitive but unclassified information, including SSI. GAO recommended that the guidance cover decisions on what information to protect with sensitive but unclassified designations; provisions for training on making designations, controlling, and sharing such information with other entities; and a review process to determine how well the program is working.[492]

To some extent approaches suggested by GAO may also apply to managing security information not covered by federal requirements. Actual application of the principles may need to be modified depending on the size and organization of the transit agency.

1. Maintaining Contract Security Information Within the Transit Agency

The transit agency should maintain contract security records within the agency using safeguards appropriate to the type of information involved. The need for security applies to transit agency employees, contractors, and auditors. Specific federal recommendations for controlling SSI were discussed in II.B.2, Federal Agencies, *supra*. General measures to ensure confidentiality of contract security records are reviewed here.

(A) Physical Security.—Transit agencies should restrict access to facilities (or portions thereof) where security information is stored, as well as visual inspection of facilities that could reveal security information. To the extent that information must be kept confidential, agencies should make sure that both hard copy and electronic systems are secure.

(B) Other Controls Within the Agency.—It may be useful to have SSI program managers/coordinators to communicate SSI responsibilities to other employees.[493] In any event, it is advisable for transit agency policy to ensure that employees who may have access to security information, either by creating it or handling it, understand the legal requirements associated with that information. It may be useful to ensure that such employees are knowledgeable enough to recognize what might be SSI or other security information and refer such information to the agency's designated SSI office(r).[494]

A number of measures are available to put employees on notice of security requirements and the penalties for violating those requirements. These include requiring NDAs and/or background checks for employees with access to security information, requiring tracking of the location of security documents, restricting copying, and prohibiting removal of security documents from transit agency premises or project location. Background checks must comply with federal law. NDAs often include or incorporate by reference the security measures that security information is subject to. In addition to standard agreement provisions such as choice of laws, an NDA may also include some or all of the following elements: recitation of the confidential nature of information to be disclosed; categories of information to be covered by confidentiality requirements; requirements for protecting SSI and penalties for violating those requirements; marking requirements and how to treat documents so marked; restricted uses allowed for information provided under the NDA; restricted access to information provided under the NDA; standard of care for information provided under the NDA; requirements for responding to any requests directed to recipient for information provided under the NDA; setting forth the recipient's obligations to return information provided under the NDA; and reserving the disclosing party's rights to seek injunctive relief to enforce the NDA.

(C) Releasing Information to Contractors.—There are a number of steps that transit agencies may take to maintain the confidentiality of security information, including SSI. For example, the transit agency may require NDAs and criminal background checks before contractors receive bid documents, participate in site inspections, or are otherwise allowed access to agency security information.[495] Some of these measures may

---

[491] *Id*. GAO cited TSA's own Internal Security Policy Board on the importance of providing specific guidance about what material is and is not covered:

> The board concluded that essential elements of the framework [to identify, control, and protect SSI] should include, among other things, "…exacting specificity with respect to what information is covered and what is not covered. This specificity could be documented in a classification guide type format because imprecision in this area causes a significant impediment to determining SSI. Experience has shown that employees unsure as to what constitutes SSI may err on the side of caution and improperly and unnecessarily restrict information, or may err inappropriately and potentially disastrously on the side of public disclosure."

Id. at 3–4. GAO has reported that TSA has taken actions to address those GAO recommendations and has addressed the legislative mandates from the DHS Appropriations Act, 2007. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 138, at 5.

[492] U.S. GOV'T ACCOUNTABILITY OFFICE, INFORMATION SHARING: THE FEDERAL GOVERNMENT NEEDS TO ESTABLISH POLICIES AND PROCESSES FOR SHARING TERRORISM-RELATED AND SENSITIVE BUT UNCLASSIFIED INFORMATION 29 (2006), www.gao.gov/new.items/d06385.pdf (accessed Oct. 10, 2009).

[493] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 138, at 13.

[494] *See* CHANDLER, SUTHERLAND, & ELDREDGE, *supra* note 164, at 7.

[495] *See, e.g.*, VDOT requirement for Non-Disclosure Agreement and criminal background check before allowing tunnel site visit. Downtown Tunnel/Midtown Tunnel/MLK Freeway Extension Project Site Visit No. 2, www.virginiadot.org/projects/resources/hampton_roads/MTCPPPTA_SiteVisit2_Registration_rtp_080630.pdf (accessed Apr. 1, 2009); VDOT requirement for fingerprint-based Criminal History Background Checks for contractor employees who will

take place as part of the prequalification process before bids are submitted.[496] These types of requirements are common in situations where individuals have a bona fide need to know information not commonly available outside the disclosing agency.[497]

The transit agency may also require that contractors adopt specific security procedures for handling the agency's security information. Such procedures often include the requirement that the contractors designate security officers to be responsible for managing the transit agency's security information.

Transit agencies may maintain secure Web sites for storing, sharing, and distributing security-related project documentation. If so, the agencies may require prospective contractors to designate security information managers to ensure that access is limited to contractor employees who have passed required background checks and/or signed access agreements.[498]

(D) Releasing Information for Contract Reviews, Other Governmental Authorizations (including Triennial Reviews).—Contractors conducting Triennial Reviews should be familiar enough with required procedure not to ask for copies of SSI. Nonetheless, agency personnel should be aware that controlled access applies to these reviewers. Any examination of SSI should be on a need-to-know basis and conducted on site.

(E) Disposal of Security Information.—At the end of the required period for agency record retention, the transit agency should dispose of records as required by state or local law. Assuming that the transit agency has the authority to destroy the records (as opposed to being required to archive them), any documentation still deemed to be SSI/restricted security information should be destroyed securely so that the information is unusable. Contractors should be required to return any such information to the transit agency or destroy it securely when the information is no longer required for the purposes for which it was disclosed to the contractor. Under no circumstances should SSI/restricted security information be disposed of in an unsecure manner (such as leaving it in trash cans at the project site).

2. Handling FOIA Requests

Employees responsible for responding to FOIA requests may need more detailed guidance about classifying SSI than is necessary to generally educate employees about the need to protect SSI. It may be advisable to limit employees tasked with evaluating FOIA requests for SSI/restricted security information to security officers or legal counsel, regardless of which employees were originally authorized to designate the information as security sensitive. For example, TSA requires its SSI Office to review requests to release SSI, regardless of which office originally identified the information as SSI.[499]

There is a distinction between control and release of information. If part of a record constitutes SSI or otherwise protected security information, the entire record should be treated as confidential in terms of maintenance and release to contractors. However, this does not mean that the entire record is exempt from disclosure. If a request is made for a record that contains SSI or otherwise protected security information, most state laws require that to the extent feasible the sensitive portion be redacted and the remainder released (assuming no other exemption requires nondisclosure).

3. Consider Instituting Review to Determine Whether Previously Designated Security Information Should Still Be Classified as Security Information

When TSA instituted a policy of reviewing SSI documents to determine their status, 282 documents determined to be SSI in their entirety (as reported to Congress in 2006) were determined to no longer warrant such continued protection.[500] By making records publicly available once their disclosure no longer poses a security threat, periodic review of records categorized as SSI or otherwise protected as security sensitive furthers the public interest in maximum disclosure consistent with public security.

Alternatives for adopting such a review procedure include periodic reviews, reviews upon request for the

handle CII/SSI under contract. RFP for Interstate 64 Widening Route 143 (east) to Route 199 (west) NEPA and Design Services, www.virginiadot.org/business/resources/RFP_I-64_Hampton_Roads.pdf.

[496] *E.g.,* The Port Authority of New York and New Jersey, Request for Pre-Qualification Information for WTC-General Site Work Via Work Order Contract, Apr. 2009, RFQ Number 18271 (issued before issuance of project RFPs, www.panynj.gov/DoingBusinessWith/contractors/pdfs/RFQI_18271.pdf; The Port Authority of New York and New Jersey, Request for Qualification Information for Greenwich Street Corridor Construction, May 2009, Contract Number WTC-224.545, www.panynj.info/DoingBusinessWith/contractors/pdfs/RFQDOC_WTC224545.pdf.

[497] For example, TSA requires a criminal background check before allowing litigants in civil proceedings with a substantial need for SSI to receive the requested SSI. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 491, at 20. The Washington Suburban Sanitary Commission (WSSC) has used background security checks before it allowed inspection of plans and drawings showing the location of water and wastewater systems and also requires background checks for applicants for new water and sewer service before the applicants are allowed access to the WSSC's electronic records management system to access plans and specifications in order to design and construct system expansions. July 31, 2007, letter from WSSC to the Maryland Attorney General, included in GANSLER, *supra* note 53.

[498] *E.g.*, The Port Authority of New York and New Jersey, Request for Pre-Qualification Information for WTC-General Site Work Via Work Order Contract, Apr. 2009, RFQ Number 18271, at 5 (III: General Requirements: L. Name and Phone Number of Security Information Manager), www.panynj.gov/DoingBusinessWith/contractors/pdfs/RFQI_18271.pdf.

[499] U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 138, at 21.

[500] *Id*. at 14.

information regardless of the age of the information, and reviews before public records are removed from active files.

4. Auditing Records Management Procedures

Developing and implementing adequate procedures for managing security information, particularly SSI, is a necessary step. However, procedures are only useful to the extent that they are actually followed.[501] Areas that may be of particular concern include maintaining a complete list of individuals authorized to access security information and being able to locate all security documents.

D. Issues to Consider in Establishing/Reviewing Security Protocol for Procurement Process

The broader areas of concern discussed in the preceding subsections may be broken down into several issues that transit agencies may wish to consider in establishing a security protocol for handling security information in the procurement process. These issues are also relevant in reviewing an existing protocol. These issues are covered in checklist format in Appendix G.

Applicability of the points raised below will depend in part on the size and organizational structure of the transit agency. The job descriptions of personnel who appropriately carry out functions identified below will also vary according to agency size and organizational structure. Agency counsel should of course review the suitability of adopting any of these approaches.

1. Record Retention Requirements

- Federal, state, and local (whichever is most stringent) records retention requirements will affect the length of time that the protocol must be observed for specific documents.
- It may be advisable to ensure that decision-makers understand the parameters of these requirements so that they can take into account the burdens that may be incurred by including various types of security information in procurement documentation.

2. Record Disclosure Requirements

- In addition to record managers, it may be useful for any personnel with control over development of contract documentation to understand the requirements of state FOIA law, so that they are aware of what information included in the procurement documentation may be subject to disclosure.
- In particular, it would be useful to understand what exemptions applicable to contract documentation, if any, may be used to protect security information, and the standards for applying those exemptions, including the need, if any, to provide substantiation of a finding of endangerment of public safety (or statutory equivalent) to support the application of an exemption.[502]

3. Relationship Between General Policy for Managing Security Information and Procurement Process

- Effectiveness of the management of security information will hinge in part on the effectiveness of the process for designating security information to begin with.
- It may be advisable to have a single point of contact for designating SSI and restricted security information, either agency-wide or for each department. DHS, for example, is required to have at least one SSI coordinator in each DHS office that handles SSI.
- It may also be advisable to ensure that the agency FOIA officer coordinates with the SSI designator/personnel.
- If the agency's legal counsel is not routinely involved in FOIA requests, it may be advisable to at least involve counsel in requests for certain types of security information.[503]
- Authority to designate need-to-know status is important to the effectiveness of security protocol.
- Need to know must have some limits to be meaningful. If most or all personnel working on a project need to know specified information, it is reasonable to question the sensitivity of the information. In addition, the more people who have access to information, the harder it is to track that access.
- Overclassifying information as SSI or restricted security information may lead to two problems: tracking system bloat and the "boy who cried wolf" syndrome.
- If the tracking system becomes too cluttered with information that is not truly sensitive, information that is truly sensitive becomes more difficult to track.

[501] The New York State Comptroller audited the Metropolitan Transportation Authority's (MTA's) controls over the dissemination of security-sensitive information for the capital projects program and found that while the MTA's guidelines provided a reasonable control framework, certain procedures were not being consistently followed. MTA took action in response to the Comptroller's recommendations. Office of the New York State Comptroller, Metropolitan Transportation Authority Controls Over Security-Sensitive Information for the Capital Projects Program, Report 2006-S-6, Sept. 6, 2006, www.osc.state.ny.us/audits/allaudits/093006/06s6.htm.

[502] State security exemptions may set forth broad categories of documents that fall within the exemption, but require a finding of public endangerment as to a specific document. For example, Maryland's statute only exempts vulnerability assessments and specified related documents to the extent that inspection would jeopardize facility security, facilitate planning of a terrorist attack, or endanger life or physical safety. *See* III.B.2, *Vulnerability Assessments*, *supra* this digest.

[503] For example, as of 2002, the Texas Department of Transportation required legal counsel review before any requests for bridge design or plans could be released to the public. TRANSTECH MANAGEMENT, INC., *supra* note 1, at App. B.

• Employees may become lax in following procedures that require tracking seemingly inconsequential information.

4. Managing Contractors' Use of Needed Security Information

• The policy should clearly establish the range of options that are available to maintain confidentiality of SSI and other security information in contract documents and otherwise available to contractors.

• Confidentiality requirements, including training, NDAs, and logs, should be applied objectively rather than on the basis of personal knowledge of the contractor.

• Even if bid/contract documents themselves are free from SSI and restricted security information, the policy should address other parts of the competitive procurement process that exposes security information, such as site visits or on-site examination of plans.

5. Taking Steps to Protect Security Information Internally

• The security protocol can be expected to include training. It is advisable that the required training covers the procurement process.

• Security requirements such as signing NDAs should be uniformly required throughout the agency, including senior level personnel.

• Requirements for tracking the location of security documents should be uniformly required throughout the agency, including senior level personnel.

• If the transit agency expects to generate restricted security information, it may be useful to distinguish under its security policy between CII/SSI and restricted security information, particularly in terms of making clear the federal penalties for making unauthorized disclosure of CII/SSI.

• Protocol should make clear that careless handling of security information may affect the ability to assert state exemptions.

• It may be advisable to audit security procedures within the agency.

6. How to Exercise Available Discretion Concerning Public Disclosure

• Depending on state law, the agency may have discretion as to whether to withhold restricted security information under state public records exemptions.

• The transit agency may consider reviewing security information to determine whether release of a specific document may cause harm, as opposed to withholding information based on document classification. Such a distinction may in fact be required under state law.

• This approach may also be possible in designating security information, including SSI.

VI. CONCLUSIONS

Historically, transit agencies have had to be mindful of confidentiality in the procurement process, perhaps most notably in maintaining the confidentiality of trade secrets and confidential business information. More recently, maintaining the confidentiality of security information, including SSI, has come to the fore. The new federal requirements for security-related information raise more complex disclosure and records management issues than those many transit agencies have traditionally faced in the procurement process.

While security information concerns are most obvious when dealing with security contracts, transit agency personnel should also be aware of the potential for security information being included in competitive bidding documents for other types of contracts. There are several major stages of the procurement process at which it is important to be cognizant of security requirements: developing the procurement documentation (whether to include SSI or restricted security information); allowing site visits and access to ancillary documents not part of the procurement documentation, either before or after contract award; responding to requests for information from parties other than bidders and contractors; and managing procurement documents. It is important that transit agencies provide the decisional infrastructure necessary for adequate consideration of security issues at those various stages.

At the bidding stage, personnel should be aware of legal requirements governing disclosure of security information to contractors, for maintaining the confidentiality of security information, and governing disclosure of security information to members of the public. Contract personnel, as well as any personnel with significant input into procurement documents, should be trained on these requirements, including the disclosure and management ramifications of including SSI/restricted security information in procurement documents. Such ramifications—which may vary depending on state law—include the possibility that the information may be disclosable under state law and the obligation to physically and electronically secure the information. Moreover, it is advisable that the need to include SSI/restricted security information in procurement documents be assessed by personnel knowledgeable about the ramifications of such inclusion.

The obligation to safeguard security information, particularly SSI, extends to contract management, and transit agencies are advised to ensure that their records management policies, including those for procurement records, are structured accordingly. In particular, it is important to ensure that existing SSI procedures, such as those required for major capital projects, are adequately coordinated with the agency's procurement and records management procedures. Procedures should

ensure that personnel with the requisite expertise, such as legal counsel or records managers, review any public record requests for documents containing SSI/restricted security information. Such personnel should be familiar with state as well as federal disclosure and records management requirements.

APPENDIX A: Federal Statutory and Regulatory Provisions

Links to citations are provided for convenience; transit agencies should verify statutory language from official sources.

Legislation

- Aviation and Transportation Security Act of 2001, Public Law (Pub. L.) No. 107–71, 115 Stat. 597, Nov. 19, 2001, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ071.107.pdf.

- Critical Infrastructures Protection Act of 2001, 42 U.S.C. 5195c [Section 1016 of USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, Oct. 26, 2001, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ056.107.pdf].

- Homeland Security Act of 2002, Pub. L. No. 107-296, 116 Stat. 2135, Nov. 25, 2002, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ296.107.pdf.

- Critical Infrastructure Information Act of 2002, 116 Stat. 2150, Subtitle B of Homeland Security Act of 2002, Pub. L. No. 107-296, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=107_cong_public_laws&docid=f:publ296.107.pdf.

- Department of Homeland Security Appropriations Act, 2006, Pub. L. No. 109–90, 119 Stat. 2064, Oct. 18, 2005, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ090.109.pdf.

- Department of Homeland Security Appropriations Act, 2007, Pub. L. No. 109–295,120 Stat. 1355, *et seq*., Oct. 4, 2006, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_public_laws&docid=f:publ295.109.pdf.

- Implementing Recommendations of the 9/11 Commission Act of 2007, §§ 1203, 1305, Pub. L. No. 110-53, 121 Stat. 266, Aug. 3, 2007, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ053.110.pdf.

- National Transit Systems Security Act of 2007 (Title XIV of the Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. No. 110-53, 121 Stat. 400 (Aug. 3, 2007)), http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ053.110.pdf.

- Openness Promotes Effectiveness in our National Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524, *et seq.,* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ175.110.pdf.

- Freedom of Information Act (FOIA), 5 U.S.C. 552, http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&TYPE=TEXT&FILE=/diska/wais/data/browse_usc/usc5.wais&start=187652&size=125475&TYPE=TEXT.

- 6 U.S.C. § 114 (Sensitive Security Information), http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc5.wais&start=187652&SIZE=125475&TYPE=PDF.

- 6 U.S.C. § 133 (Protection of voluntarily shared critical infrastructure information), http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&TYPE=TEXT&FILE=/diska/wais/data/browse_usc/usc5.wais&start=187652&size=125475&TYPE=TEXT.

- 6 U.S.C. § 1333 (National Strategy for Public Transportation Security), http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc6.wais&start=1530875&SIZE=3989&TYPE=PDF.

- 6 U.S.C. § 1334 (Security assessments and plans), http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc6.wais&start=1534870&SIZE=10422&TYPE=PDF.

- 6 U.S.C. § 1335 (Public transportation security assistance), http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc6.wais&start=1545298&SIZE=10293&TYPE=PDF.

- 6 U.S.C. § 1337 (Public transportation security training program), http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc6.wais&start=1559208&SIZE=6102&TYPE=PDF.

- 6 U.S.C. § 1343 (Security background checks of covered individuals for public transportation), http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc6.wais&start=1597129&SIZE=8342&TYPE=PDF.

- 49 U.S.C. § 5327(a)(13) (Safety and security management plan), http://frwebgate.access.gpo.gov/cgi-bin/usc.cgi?ACTION=RETRIEVE&FILE=$$xa$$busc49.wais&start=1781790&SIZE=12643&TYPE=PDF.

- 49 U.S.C. § 5330 (State safety oversight), http://frwebgate4.access.gpo.gov/cgi-bin/TEXTgate.cgi?WAISdocID=314704359398+0+1+0&WAISaction=retrieve.

- 49 U.S.C. § 40119(b) (Security and research and development activities: disclosure), http://frwebgate3.access.gpo.gov/cgi-bin/TEXTgate.cgi?WAISdocID=31734223381+0+1+0&WAISaction=retrieve.

Regulations/Executive Memoranda/Guidance/Project Agreements

Department of Homeland Security

- Procedures for Handling Critical Infrastructure Information, 6 C.F.R. Part 29.

- 49 C.F.R. Part 1515, Appeal and Waiver Procedures for Security Threat Assessments for Individuals, www.access.gpo.gov/nara/cfr/waisidx_08/49cfr1515_08.html [TSA suggests this as a model for appeal and waiver process—"Status," www.tsa.dhs.gov/assets/pdf/guidance_employee_background_checks.pdf].

- 49 C.F.R. Part 1520, Protection of Sensitive Security Information, www.access.gpo.gov/nara/cfr/waisidx_08/49cfr1520_08.html.

- 49 C.F.R. § 1572.103, Disqualifying criminal offenses http://edocket.access.gpo.gov/cfr_2008/octqtr/pdf/49cfr1572.103.pdf [TSA suggests this as a model for background checks—"Additional Guidance on Background Checks Redress and Immigration," www.tsa.dhs.gov/assets/pdf/guidance_employee_background_checks.pdf].

- 49 C.F.R. Part 1580, Rail Transportation Security, Subpart C—Passenger Rail Including Passenger Railroad Carriers, Rail Transit Systems, Tourist, Scenic, Historic and Excursion Operators, and Private Cars, http://frwebgate4.access.gpo.gov/cgi-bin/TEXTgate.cgi?WAISdocID=315211406194+17+1+0&WAISaction=retrieve.

Department of Justice

- Guide to the Freedom of Information Act (June 2009), www.justice.gov/oip/foia_guide09.htm.

Department of Transportation

- Public Availability of Information, 49 C.F.R. Part 7, www.access.gpo.gov/nara/cfr/waisidx_08/49cfr7_08.html.

- Protection of Sensitive Security Information, 49 C.F.R. Part 15, www.access.gpo.gov/nara/cfr/waisidx_08/49cfr15_08.html.

- Record Retention, 49 C.F.R. §§ 18.36(i)(11); 18.42, www.access.gpo.gov/nara/cfr/waisidx_08/49cfr18_08.html.

Federal Transit Administration

- 49 C.F.R. Part 659, Rail Fixed Guideway Systems; State Safety Oversight, www.access.gpo.gov/nara/cfr/waisidx_08/49cfr659_08.html.

- FTA Master Agreement, October 1, 2009, Section 8. Reporting, Record Retention, and Access, www.fta.dot.gov/documents/16-Master.pdf.

- FTA Master Agreement, Section 37. Protection of Sensitive Security Information, www.fta.dot.gov/documents/16-Master.pdf.

- FTA Circular 5800.1, *Safety and Security Management Guidance for Major Capital Projects* (August 1, 2007), www.fta.dot.gov/laws/circulars/leg_reg_6930.html.

- FTA Circular 4220.1F, *Third Party Contracting Guidance* (November 1, 2008, and amendments thereto), www.fta.dot.gov/laws/circulars/leg_reg_8641.html.

- *Sensitive Security Information (SSI): Designation, Markings, and Control* (Resource Document for Transit Agencies), March 2009, http://transit-safety.volpe.dot.gov/publications/order/singledoc.asp?docid=968.

- FOIA Requests, www.fta.dot.gov/about/about_FTA_186.html.

- 49 C.F.R. Part 659 Reference Guide, June 22, 2005, http://transit-safety.volpe.dot.gov/publications/sso/49CFRPart659_FinalRule/49CFR659_Reference_Guide.pdf.

- TSA/FTA Security and Emergency Action Items for Transit Agencies, Document Control, http://transit-safety.volpe.dot.gov/security/SecurityInitiatives/ActionItems/actionlist.asp#Document_Control.

- Memorandum of January 21, 2009—Freedom of Information Act, 74 Fed. Reg. 4683, January 26, 2009, http://edocket.access.gpo.gov/2009/pdf/E9-1773.pdf.

APPENDIX B: State Public Records/Freedom of Information Laws

Links to citations are provided for convenience; transit agencies should verify statutory language from official sources.

Alabama: Ala. Code, § 36-12-40, http://alisondb.legislature.state.al.us/acas/codeofalabama/1975/36-12-40.htm.

Every citizen has a right to inspect and take a copy of any public writing of this state, except as otherwise expressly provided by statute. [Balance of provision sets forth exemptions from right to inspect.].

Alaska: Alaska Stat/ Title 40. Public Records and Recorders: Chapter 25. Public Record Disclosures, www.touchngo.com/lglcntr/akstats/Statutes/Title40/Chapter25.htm; Alaska Stat. 40.25.110. Public Records Open to Inspection and Copying; Fees, www.touchngo.com/lglcntr/akstats/Statutes/Title40/Chapter25/Section110.htm.

Arizona: Ariz. Rev. Stat. Title 39, Chapter 1, Public Records, www.azleg.state.az.us/ArizonaRevisedStatutes.asp?Title=39; Ariz. Rev. Stat. 39-121. Inspection of public records, www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/39/00121.htm&Title=39&DocType=ARS.

Arkansas:[504] Ark. Stat. Ann. § 25-19-105. Examination and copying of public records, http://ag.arkansas.gov/pdfs/foia-ocr.pdf ;

(a)(1)(A) Except as otherwise specifically provided by this section or bylaws specifically enacted to provide otherwise, all public records shall be open to inspection and copying by any citizen of the State of Arkansas during the regular business hours of the custodian of the records….

***

(f)(1) No request to inspect, copy, or obtain copies of public records shall be denied on the ground that information exempt from disclosure is commingled with nonexempt information.

(2) Any reasonably segregable portion of a record shall be provided after deletion of the exempt information.

(3) The amount of information deleted shall be indicated on the released portion of the record and, if technically feasible, at the place in the record where the deletion was made.

California: California Public Records Act, Government Code Section 6250-6270, www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6250-6270: Section 6253 [inspection and copying requirements]; Section 6253.31. Notwithstanding any contract term to the contrary, a contract entered into by a state or local agency subject to this chapter, including the University of California, that requires a private entity to review, audit, or report on any aspect of that agency shall be public to the extent the contract is otherwise subject to disclosure under this chapter.

Colorado: Colorado Open Records Act, Colo. Rev. Stat. Title 24, Article 72, Part 2, INSPECTION, COPYING, OR PHOTOGRAPHING, www.michie.com/colorado/lpext.dll?f=templates&fn=main-h.htm&cp=.

Connecticut: Connecticut Freedom of Information Act, www.state.ct.us/foi/2003FOIA/Full%202003%20FOI%20Act.htm.

Delaware: Freedom of Information Act, 29 Del. Code § 10001, http://delcode.delaware.gov/title29/c100/index.shtml.

District of Columbia: D.C. Code, Title 2, Ch. 5, Subch. II, Freedom of Information, §§ 2-531 to 2-540, http://government.westlaw.com/linkedslice/default.asp?SP=DCC-1000.

Florida: Public Records Statute, §§ 119.01 *et seq.*, www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&URL=Ch0119/titl0119.htm&StatuteYear=2008&Title=%2D%3E2008%2D%3EChapter%20119.

[504] Additional reference: Open Government Guide: www.rcfp.org/ogg/index.php?op=browse&state=AR.

Georgia: Ga. Code Ann., Article 4, Inspection of Public Records, http://sos.georgia.gov/Archives/who_are_we/rims/best_practices_resources/open_records_act.htm#50-18-72; 50-18-70. Inspection of public records; printing of computerized indexes of county real estate deed records; time for determination of whether requested records are subject to access, http://sos.georgia.gov/Archives/who_are_we/rims/best_practices_resources/open_records_act.htm#50-18-70.

Hawaii: Uniform Information Practices Act, Haw. Rev. Stat. § 92F, www.state.hi.us/oip/uipa.html; www.state.hi.us/oip/UIPA%20Manual%205aug08.pdf.

Idaho: Idaho Code §§ 9-337 to 9-347, www.legislature.idaho.gov/idstat/Title9/T9CH3.htm.

Illinois: Freedom of Information Act, 5 Ill. Comp. Stat. 140, www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=85&ChapAct=5%20ILCS%20140/&ChapterID=2&ChapterName=GENERAL+PROVISIONS&ActName=Freedom+of+Information+Act.

Indiana: Ind. Code 5-14-3, Chapter 3. Access to Public Records; Ind. Code 5-14-3-3, Right to inspect and copy public agency records; electronic data storage; use of information for commercial purposes; contracts [Refusing to state purpose of request not grounds for denying request, unless another statute requires such condition], www.in.gov/legislative/ic/code/title5/ar14/ch3.html.

Iowa: Examination of Public Records (Open Records), Iowa Code Chapter 22, http://coolice.legis.state.ia.us/Cool-ICE/default.asp?category=billinfo&service=IowaCode&ga=83.

Kansas: Open Records Act, Kan. Stat. Ann. 45-215 through 45-223. Accessible from www.kslegislature.org/legsrv-statutes/index.do.

Kentucky: Open Records, Ky. Rev. Stat. 61.870-61.884 www.lrc.state.ky.us/krs/061-00/chapter.htm, 61.871 Policy of Ky. Rev. Stat. 61.870 to 61.884—Strict construction of exceptions of Ky. Rev. Stat. 61.878, www.lrc.state.ky.us/krs/061-00/871.PDF. The General Assembly finds and declares that the basic policy of Ky. Rev. Stat. 61.870 to 61.884 is that free and open examination of public records is in the public interest and the exceptions provided for by Ky. Rev. Stat. 61.878 or otherwise provided by law shall be strictly construed, even though such examination may cause inconvenience or embarrassment to public officials or others. Ky. Rev. Stat. 61.872 Right to inspection—Limitation, www.lrc.ky.gov/krs/061%2D00/872.pdf.

Louisiana: Public Records and Recorders, La. Rev. Stat. Ann. Title 44, www.legis.state.la.us/lss/lss.asp?folder=118.

Maine: Freedom of Access Act, www.mainelegislature.org/legis/statutes/1/title1ch13sec0.html.

Maryland:[505] Public Information Act, §§ 10-611 through 10-630, www.oag.state.md.us/opengov/Appendix_C.pdf.

Massachusetts:[506] Public Records Law, Mass. Gen. Laws c. 4, § 7(26) [definition and exemptions], www.mass.gov/legis/laws/mgl/4/4-7.htm; Mass. Gen. Laws c. 66, § 10(a), www.mass.gov/legis/laws/mgl/66-10.htm.

Michigan: Freedom of Information Act, Act 442 of 1976, www.legislature.mi.gov/(S(m4by0iqwcqquvpauqp4z1eap))/mileg.aspx?page=getobject&objectname=mcl-act-442-of-1976.

Minnesota: Minnesota Government Data Practices Act, Minnesota Statutes, 2008, Chapter 13, www.revisor.leg.state.mn.us/data/revisor/statute/2008/013/2008-13.pdf.

[505] *See* MARYLAND PUBLIC INFORMATION ACT MANUAL (11th ed. 2008), www.oag.state.md.us/Opengov/pia.htm.

[506] *See* A GUIDE TO THE MASSACHUSETTS PUBLIC RECORDS LAW, www.sec.state.ma.us/pre/prepdf/guide.pdf.

Mississippi: Mississippi Public Records Act, Title 25, Chapter 61, Mississippi Code of 1972, www.ethics.state.ms.us/ethics/ethics.nsf/PageSection/A_records_entire_pub_rec_act/$FILE/Public%20Records%20Act.htm?OpenElement.

Missouri: Sunshine Law, Mo. Rev. Stat. §§ 610.010-.200, http://ago.mo.gov/sunshinelaw/chapter610.htm.

Montana: Public Records Act, Mont. Code Ann. §§ 2-6-101 through 2-6-112, http://data.opi.mt.gov/bills/mca_toc/2_6_1.htm.

Nebraska: Public records; free examination; memorandum and abstracts; copies; fees. Neb. Rev. Stat. § 84-712, http://uniweb.legislature.ne.gov/laws/statutes.php?statute=s8407012000.

Nevada: Public Records, Nev. Rev. Stat. 239.001 *et seq.*, www.leg.state.nv.us/NRS/NRS-239.html#NRS239Sec001.

New Hampshire: Access to Governmental Records and Meetings N.H. Rev. Stat. Ann., Chapter 91-A, www.gencourt.state.nh.us/rsa/html/NHTOC/NHTOC-VI-91-A.htm.

New Jersey: N.J. Stat. Ann. 47:1A, http://www.njleg.state.nj.us/2000/Bills/PL01/404_.PDF.

New Mexico: Inspection of Public Records Act, 14-2-4 N.M. Stat. Ann. 1978, www.conwaygreene.com/nmsu/lpext.dll?f=templates&fn=main-h.htm&2.0.

New York: Freedom of Information Law, Sections 84–90 of Article 6, Public Officers Law, http://public.leginfo.state.ny.us/menugetf.cgi [Select PBO, then Article 6].

North Carolina: Public Records Law, General Statute 132, www.ncleg.net/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_132.html.

North Dakota: Access to Public Records, N.D. Cent. Code § 44-04-18, www.legis.nd.gov/cencode/t44c04.pdf.

Ohio:[507] Availability of public records for inspection and copying, Ohio Rev. Code § 149.43, http://codes.ohio.gov/orc/149.43.

Oklahoma: Oklahoma Open Records Act, 51 Okla. Stat. §§ 24A.1 *et seq.*, www.lsb.state.ok.us/osstatuestitle.html.

Oregon: Public Records Law, Or. Rev. Stat. Chapter 192; Inspection of Public Records, Or. Rev. Stat. §§ 192.410 to 192.505, www.leg.state.or.us/ors/192.html.

Pennsylvania: Right-to-Know Law, 65 Pa. Stat. § 67.101 *et seq*., www.dced.state.pa.us/public/oor/pa_righttoknowlaw.pdf.

Rhode Island: Access to Open Records Act, R.I. Gen. Laws, Chapter 38-2, www.rilin.state.ri.us/statutes/title38/38-2/INDEX.HTM.

South Carolina: Freedom of Information Act, S.C. Code Ann. § 30-4-10 *et seq*., www.scstatehouse.gov/code/t30c004.htm.

South Dakota: S.D. Codified Laws, § 1-27-1 *et seq*., http://legis.state.sd.us/statutes/DisplayStatute.aspx?Type=Statute&Statute=1-27.

Tennessee: Tennessee Open Records Act, Tenn. Code Ann. 10-7-101, www.michie.com/tennessee/lpext.dll?f=templates&fn=main-h.htm&cp=.

---

[507] *See* RICHARD CORDRAY & MARY TAYLOR, OHIO SUNSHINE LAWS: AN OPEN GOVERNMENT RESOURCE MANUAL 2009, www.ohioattorneygeneral.gov/getattachment/e4872b55-8b91-4257-8e4f-ba78f0f44422/2009-Sunshine-Laws-Manual.aspx (accessed Oct. 10, 2009).

Texas: Texas Public Information Act, Tex. Gov't Code Ann. § 552.001 *et seq*., http://www.tsl.state.tx.us/agency/customer/pia.html.

Utah: Government Records Access and Management Act, Utah Code Ann. § 63G-2-101 *et seq*., http://le.utah.gov/~code/TITLE63G/63G02.htm.

Vermont:[508] Public Records Act, 1 Vt. Stat. Ann. §§ 315–320, www.leg.state.vt.us/statutes/fullchapter.cfm?Title=01&Chapter=005.

Virginia: Virginia Freedom of Information Act, Va. Code Ann. § 2.2-3700 *et seq*., http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+TOC02020000037000000000000.

Washington: Public Records Act, Chapter 42.56 Wash. Rev. Code, http://apps.leg.wa.gov/rcw/default.aspx?cite=42.56; Chapter 44-14 WAC Public Record Act—Model Rules, http://apps.leg.wa.gov/wac/default.aspx?cite=44-14.

West Virginia: Freedom of Information, W. Va. Code, www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=29b.

Wisconsin:[509] Wis. Stat. §§ 19.31-19.37, www.legis.state.wi.us/statutes/Stat0019.pdf.

Wyoming: Public Records, Wyo. Stat. §§ 16-4-201 through 14-4-205, http://legisweb.state.wy.us/statutes/titles/Title16/T16CH4AR2.htm.

[508] Legislative analysis, www.leg.state.vt.us/REPORTS/07PublicRecords/Public%20Records%20Requirements%20in%20Vermont.pdf.

[509] Attorney General J.B. Van Hollen, Wisconsin Public Records Law, Wis. Stat. §§ 19.31–19.39, Compliance Outline, Aug. 2007, www.doj.state.wi.us/dls/OMPR/2009OMCG-PRO/2009_Pub_Rec_Outline.pdf.

APPENDIX C: Security Exemptions to State Public Records/Freedom of Information Laws[510]

The following exemptions are security exemptions unless otherwise noted. Additional exemptions are included for illustrative purposes only. Transit agencies should research their own state law (including the open records statutes cited in Appendix B) for other exemptions that may be used to retain confidentiality of security information. Such exemptions include those that include by reference specific federal exemptions or federal exemptions in general, as well as exemptions—such as the deliberative process exemption—that may protect security-related information on procedural grounds. Links to citations are provided for convenience; transit agencies should verify statutory language from official sources.

Alabama: Ala. Code, § 36-12-40, http://alisondb.legislature.state.al.us/acas/codeofalabama/1975/36-12-40.htm.

Notwithstanding the foregoing, records concerning security plans, procedures, assessments, measures, or systems, and any other records relating to, or having an impact upon, the security or safety of persons, structures, facilities, or other infrastructures, including without limitation information concerning critical infrastructure (as defined at 42 U.S.C. § 5195c(e) as amended) and critical energy infrastructure information (as defined at 18 C.F.R. § 388.113(c)(1) as amended) the public disclosure of which could reasonably be expected to be detrimental to the public safety or welfare, and records the disclosure of which would otherwise be detrimental to the best interests of the public shall be exempted from this section. Any public officer who receives a request for records that may appear to relate to critical infrastructure or critical energy infrastructure information, shall notify the owner of such infrastructure in writing of the request and provide the owner an opportunity to comment on the request and on the threats to public safety or welfare that could reasonably be expected from public disclosure on the records.

Alaska: Alaska Stat. 40.25.120. Public Records; Exceptions; Certified Copies, www.touchngo.com/lglcntr/akstats/Statutes/Title40/Chapter25/Section120.htm.

Arizona: Ariz. Rev. Stat. 39-126. Federal risk assessments of infrastructure; confidentiality [specifies "critical energy, water or telecommunications infrastructure"], www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/39/00126.htm&Title=39&DocType=ARS.

Arkansas: Ark. Code Ann. § 25-19-105. Examination and copying of public records, http://ag.arkansas.gov/pdfs/foia-ocr.pdf.

(b) It is the specific intent of this section that the following shall not be deemed to be made open to the public under the provisions of this chapter:

***

(9)(A) Files that if disclosed would give advantage to competitors or bidders and records maintained by the Arkansas Economic Development Commission related to any business entity's planning, site location, expansion, operations, or product development and marketing, unless approval for release of those records is granted by the business entity.

***

(16)(A) Records, including analyses, investigations, studies, reports, recommendations, requests for proposals, drawings, diagrams, blueprints, and plans containing information relating to security for any public water system.

(B) The records shall include:

(i) Risk and vulnerability assessments;

(ii) Plans and proposals for preventing and mitigating security risks;

(iii) Emergency response and recovery records;

(iv) Security plans and procedures; and

(v) Any other records containing information that if disclosed might jeopardize or compromise efforts to secure and protect the public water system.

(C) This subdivision (b)(16) shall expire on July 1, 2007.

[510] Some of these provisions exclude certain security-related information from the definition of public record altogether. GANSLER, *supra* note 53.

[According to the Arkansas Attorney General, the Homeland Security Information Act, A.C.A. 12-75-subch.1 (note) (Act 1366 of 2003) shields certain terrorism threat assessments, plans, operational policies or procedures, and training developed or maintained by "emergency service agencies" and records received from federal government and other states and cities if shielded in those jurisdictions. www.arkansasag.gov/pdfs/FOIA-Seminar-2007.ppt.].

California: Government Code, Article 1, General Provisions, Section 6254 [exemptions]

* * *

(k) Records, the disclosure of which is exempted or prohibited pursuant to federal or state law, including, but not limited to, provisions of the Evidence Code relating to privilege.

* * *

(p) Records of state agencies related to activities governed by Chapter 10.3 (commencing with Section 3512), Chapter 10.5 (commencing with Section 3525), and Chapter 12 (commencing with Section 3560) of Division 4, that reveal a state agency's deliberative processes, impressions, evaluations, opinions, recommendations, meeting minutes, research, work products, theories, or strategy, or that provide instruction, advice, or training to employees who do not have full collective bargaining and representation rights under these chapters. Nothing in this subdivision shall be construed to limit the disclosure duties of a state agency with respect to any other records relating to the activities governed by the employee relations acts referred to in this subdivision.

* * *

(aa) A document prepared by or for a state or local agency that assesses its vulnerability to terrorist attack or other criminal acts intended to disrupt the public agency's operations and that is for distribution or consideration in a closed session.

(ab) Critical infrastructure information, as defined in Section 131(3) of Title 6 of the United States Code, that is voluntarily submitted to the California Emergency Management Agency for use by that office, including the identity of the person who or entity that voluntarily submitted the information. As used in this subdivision, "voluntarily submitted" means submitted in the absence of the office exercising any legal authority to compel access to or submission of critical infrastructure information. This subdivision shall not affect the status of information in the possession of any other state or local governmental agency.

www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6250-6270.

6254.15 [exemption from disclosure requirements for corporate proprietary information including trade secrets].

6254.23. Nothing in this chapter or any other provision of law shall require the disclosure of a risk assessment or railroad infrastructure protection program filed with the Public Utilities Commission, the Director of Homeland Security, and the Office of Emergency Services pursuant to Article 7.3 (commencing with Section 7665) of Chapter 1 of Division 4 of the Public Utilities Code.

6255 [requirement to justify withholding under exemption].

6257.5 [purpose for request not relevant].

6259 [court order to disclose improperly withheld records].

California Public Records Act, Government Code, Article 2, Other Exemptions from Disclosure, Section 6275–6276.48 www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6275-6276.48 [review for relevance].

6254.5. [Disclosure of exempt public record is waiver, not applicable to a number of waivers, including public records: Made to any governmental agency which agrees to treat the disclosed material as confidential.].

Colorado: Colorado Open Records Act, Colo. Rev. Stat. Title 24, Article 72, Part 2, 24-72-204. Allowance or denial of inspection—grounds—procedure—appeal—definitions. [Exemption from disclosure for inspections contrary to state law; federal law; contracts for security to remain open, except to extent they contain details of security arrangements, such details may be withheld if disclosure found contrary to public interest; deliberative process records may be withheld if disclosure found contrary to public interest, but with explanation of why document is privileged and why disclosure would cause substantial injury to public interest.], www.michie.com/colorado/lpext.dll?f=templates&fn=main-h.htm&cp=.

Connecticut: Connecticut Freedom of Information Act, Sec. 1-210(b). Exempt records; (b)(19) Records when there are reasonable grounds to believe disclosure may result in a safety risk, including the risk of harm to any person, any government-owned or -leased institution or facility or any fixture or appurtenance and equipment attached to, or contained in, such institution or facility, except that such records shall be disclosed to a law enforcement agency upon the request of the law enforcement agency. [Includes security manuals, training manu-

als describing security procedures, and emergency plans.], www.state.ct.us/foi/2003FOIA/Full%202003%20FOI%20Act.htm.

Delaware: 29 Del. Code § 10002(g)(16), http://delcode.delaware.gov/title29/c100/index.shtml.

District of Columbia: D.C. Code Ann. § 2-534(a)(10), http://government.westlaw.com/linkedslice/default.asp?SP=DCC-1000.

Florida: Fla. Stat. § 119.071(1) [exemption for bids/proposals until agency decision is made], (3)(a) [security], www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0119/SEC071.HTM&Title=-%3E2008-%3ECh0119-%3ESection%20071#0119.071.

Georgia: Ga. Code Ann. § 50-18-72(a) [public disclosure not required for records in this category] (1) [specifically required by federal government to be kept confidential], (15)(A)[security information in specified context, covers security plans and vulnerability assessments]; (b) [public records requirements do not apply to records in this category] (1) [trade secrets required to be submitted to government], http://sos.georgia.gov/Archives/who_are_we/rims/best_practices_resources/open_records_act.htm#50-18-72.

Hawaii: Haw. Rev. Stat. § 92F-13(3) [government records that, by their nature, must be confidential in order for the government to avoid the frustration of a legitimate government function], www.state.hi.us/oip/uipa.html#92F13.

Idaho: Idaho Code § 9-340A(1) [exemptions specifically provided for in federal or state law], www.legislature.idaho.gov/idstat/Title9/T9CH3SECT9-340A.htm; Idaho Code § 9-340B(4)(b) [building records, only when disclosure would compromise public safety], www.legislature.idaho.gov/idstat/Title9/T9CH3SECT9-340B.htm.

Illinois: 5 Ill. Comp. Stat. 140/7(1)(a), (f), (g), (h) [proposal and bid information that could impede fair procurement if disclosed before award], (k), (ff) [directly relates to security portions of RTA/St. Clair County Transit District system safety program plans], (ll), www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=85&ChapAct=5%20ILCS%20140/&ChapterID=2&ChapterName=GENERAL+PROVISIONS&ActName=Freedom+of+Information+Act.

Indiana: Ind. Code § 5-14-3-4 (a) [may not be disclosed except under court order] (1)-(5); (b) [excepted from disclosure at agency's discretion] (6), (10), (19) [includes vulnerability assessments if disclosure likely to have reasonable likelihood of threatening public safety], www.in.gov/legislative/ic/code/title5/ar14/ch3.html.

Iowa: Iowa Code § 22.7. Confidential Records. 45 [critical asset protection plan]; 50 [security procedures, emergency preparedness, including vulnerability assessments]. http://coolice.legis.state.ia.us/Cool-ICE/default.asp?category=billinfo&service=IowaCode&ga=83#22.7.

Kansas: Kan. Stat. Ann. § 45-221(a)(45), accessible from www.kslegislature.org/legsrv-statutes/index.do.

Kentucky: Ky. Rev. Stat. 61.878 Certain public records exempted from inspection except on order of court—Restriction of state employees to inspect personnel files prohibited. (m), www.lrc.state.ky.us/krs/061-00/878.PDF:

(1) The following public records are excluded from the application of KRS 61.870 to 61.884 and shall be subject to inspection only upon order of a court of competent jurisdiction, except that no court shall authorize the inspection by any party of any materials pertaining to civil litigation beyond that which is provided by the Rules of Civil Procedure governing pretrial discovery:

***

(j) Preliminary recommendations, and preliminary memoranda in which opinions are expressed or policies formulated or recommended;

(k) All public records or information the disclosure of which is prohibited by federal law or regulation;

(l) Public records or information the disclosure of which is prohibited or restricted or otherwise made confidential by enactment of the General Assembly;

(m) 1. Public records the disclosure of which would have a reasonable likelihood of threatening the public safety by exposing a vulnerability in preventing, protecting against, mitigating, or responding to a terrorist act and limited to:

a. Criticality lists resulting from consequence assessments;
b. Vulnerability assessments;
c. Antiterrorism protective measures and plans;
d. Counterterrorism measures and plans;
e. Security and response needs assessments;
f. Infrastructure records that expose a vulnerability referred to in this subparagraph through the disclosure of the location, configuration, or security of critical systems, including public utility critical systems. These critical systems shall include but not be limited to information technology, communication, electrical, fire suppression, ventilation, water, wastewater, sewage, and gas systems;
g. The following records when their disclosure will expose a vulnerability referred to in this subparagraph: detailed drawings, schematics, maps, or specifications of structural elements, floor plans, and operating, utility, or security systems of any building or facility owned, occupied, leased, or maintained by a public agency; and
h. Records when their disclosure will expose a vulnerability referred to in this subparagraph and that describe the exact physical location of hazardous chemical, radiological, or biological materials.
***

3. On the same day that a public agency denies a request to inspect a public record for a reason identified in this paragraph, that public agency shall forward a copy of the written denial of the request, referred to in KRS 61.880(1), to the executive director of the Office for Security Coordination and the Attorney General.

4. Nothing in this paragraph shall affect the obligations of a public agency with respect to disclosure and availability of public records under state environmental, health, and safety programs.

(4) If any public record contains material which is not excepted under this section, the public agency shall separate the excepted and make the nonexcepted material available for examination.
(5) The provisions of this section shall in no way prohibit or limit the exchange of public records or the sharing of information between public agencies when the exchange is serving a legitimate governmental need or is necessary in the performance of a legitimate government function.

Louisiana: La. Rev. Stat. Ann. §§ 44:3.1, Certain records pertaining to terrorist-related activity, www.legis.state.la.us/lss/lss.asp?doc=206916; § 44:23.1, Department of Transportation and Development; exception for certain sensitive security information or critical infrastructure information, www.legis.state.la.us/lss/lss.asp?doc=631240.

Maine: 1 Me. Rev. Stat. Ann. § 402.3.L, www.mainelegislature.org/legis/statutes/1/title1sec402.html.

Maryland: M.S.A. § 10-618(j), Discretionary Denials: Public Security. [Custodian may deny disclosure if custodian believes disclosure would be contrary to public interest.] www.oag.state.md.us/opengov/Appendix_C.pdf.

Massachusetts: Mass. Gen. Laws c. 4, § 7, cl. 26 (a), (b), (d), (g), (h) [bids and proposal before bid closing, agency deliberations prior to contract award], (n) [includes vulnerability assessments, allows record custodian discretion not inherent in other statutory exception under Massachusetts law.[511]] www.mass.gov/legis/laws/mgl/4/4-7.htm.

Michigan: Freedom of Information Act, Act 442 of 1976, Mich. Comp. Laws § 15.243(1)(y), www.legislature.mi.gov/(S(m4by0iqwcqquvpauqp4z1eap))/mileg.aspx?page=getObject&objectName=mcl-15-243.

Minnesota: No specific security exemption. Does contain specific exemption for transportation projects during bidding process. www.revisor.leg.state.mn.us/data/revisor/statute/2008/013/2008-13.72.pdf.

Mississippi: No specific security exemption.

Missouri: Mo. Rev. Stat. § 610.021(18), (19), http://ago.mo.gov/sunshinelaw/chapter610.htm#header7 [In 2008 the security exemptions were extended through December 31, 2012. http://ago.mo.gov/pdf/MissouriSunshineLaw.pdf, pp. 54, 55.].

Montana: No specific security exemption.

[511] A GUIDE TO THE MASSACHUSETTS PUBLIC RECORDS LAW 23–24, www.sec.state.ma.us/pre/prepdf/guide.pdf.

Nebraska: Neb. Rev. Stat. § 84-712.05(8), http://uniweb.legislature.ne.gov/laws/statutes.php?statute=s8407012005. [Note discretionary nature.[512]].

Nevada: Nev. Rev. Stat. § 239C.210, 220, www.leg.state.nv.us/NRS/NRS-239C.html#NRS239CSec210.

New Hampshire: N.H. Rev. Stat. Ann., § 91-A:5, VI, www.gencourt.state.nh.us/rsa/html/VI/91-A/91-A-5.htm.

New Jersey: N.J. Stat. Ann. §§ 47:1A, http://www.njleg.state.nj.us/2000/Bills/PL01/404_.PDF.

New Mexico: N.M. Stat. Ann. § 14-2-1(A)(8), www.conwaygreene.com/nmsu/lpext.dll?f=templates&fn=main-h.htm&2.0.

New York: N.Y. Pub. Off. § 87(2)(f), (i) Freedom of Information Law, § 87.2.(a) [specifically exempted by other law], (d) [trade secret/commercial information], (f) [endanger life or safety], (g) [certain inter-agency or intra-agency materials] of Article 6, Public Officers Law, http://public.leginfo.state.ny.us/menugetf.cgi [Select PBO, then Article 6].

North Carolina: N.C. Gen. Stat. § 132.1.7, www.ncleg.net/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_132.html. Note: § 132.1.7(c): "Information relating to the general adoption of public security plans and arrangements, and budgetary information concerning the authorization or expenditure of public funds to implement public security plans and arrangements, or for the construction, renovation, or repair of public buildings and infrastructure facilities shall be public records. (2001[ ]516, s. 3; 2003[ ]180, s. 1.)".

North Dakota: N.D. Cent. Code §§ 44-04-24, Security system plan – Exemption; 44-04-25, Public health and security plans – Exemption, www.legis.nd.gov/cencode/t44c04.pdf.

Ohio: Ohio Rev. Code §§ 149.433, Exempting security and infrastructure records, http://codes.ohio.gov/orc/149.433.

Oklahoma: 51 Okla. Stat. § 24A.28, www.lsb.state.ok.us/osstatuestitle.html.

Oregon: No security exemption that would apply to transit facilities.

Pennsylvania: 65 Pa. Stat. § 67.708(b)(2) and (3), www.dced.state.pa.us/public/oor/pa_righttoknowlaw.pdf.

Rhode Island: No specific security exemption.

South Carolina: S.C. Code Ann. § 30-4-45, www.scstatehouse.gov/code/t30c004.htm.

South Dakota: No specific security exemption.

Tennessee: Tenn. Code Ann. § 10-7-503(e); § 10-7-504(a)(21).

Texas: Texas Homeland Security Act, Tex. Gov't Code Ann. §§ 418.177, 418.181, www.statutes.legis.state.tx.us/SOTWDocs/GV/pdf/GV.418.pdf , material exempted from disclosure under Texas Public Information Act, Tex. Gov't Code Ann. § 552.101.

Utah: Utah Code Ann. § 63-2-106, www.le.utah.gov/UtahCode/getCodeSection?code=63G-2-106.

Vermont: 1 Vt. Stat. Ann. § 317(c)(25), www.leg.state.vt.us/statutes/fullchapter.cfm?Title=01&Chapter=005.

Virginia: Va. Code § 2.2-3705.02 Exclusions to application of chapter; records relating to public safety, http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+2.2-3705.2.

[512] Op. Att'y. Gen. No. 94080 (Oct. 14, 1994), http://www.ago.ne.gov/agopinions/details.htm?searchStr=1&_search_id=1663.

Washington: Wash. Rev. Code § 4 2.56.420 Security, http://apps.leg.wa.gov/RCW/default.aspx?cite=42.56.420.

West Virginia: W. Va. Code § 28B-1-4(9), (10), (14), (15), www.legis.state.wv.us/WVCODE/ChapterEntire.cfm?chap=29b.

Wisconsin: Wis. Stat. § 19.36(9).

Wyoming: Wyo. Stat. § 16-4-203(b)(vi), http://legisweb.state.wy.us/statutes/titles/Title16/T16CH4AR2.htm.

APPENDIX D: State Records Management Laws

Links to citations are provided for convenience; transit agencies should verify statutory language from official sources.

Alabama:[513] Public Records, Chapter 13 of Title 41, www.legislature.state.al.us/CodeofAlabama/1975/coatoc.htm.

Alaska: Alaska Statutes, Title 40, Chapter 21, Management and Preservation of Public Records, www.touchngo.com/lglcntr/akstats/Statutes/Title40/Chapter21.htm.

Arizona: Ariz. Rev. Stat. § 39-121.01. Definitions; maintenance of records; copies, printouts, or photographs of public records; examination by mail; index, www.azleg.gov/FormatDocument.asp?inDoc=/ars/39/00121-01.htm&Title=39&DocType=ARS; Ariz. Rev. Stat. Title 41, Chapter 8, Article 3, Arizona State Library, Archives and Public Records, www.azleg.state.az.us/ArizonaRevisedStatutes.asp?Title=41; Ariz. Rev. Stat. § 41-1346, www.azleg.state.az.us/FormatDocument.asp?inDoc=/ars/41/01346.htm&Title=41&DocType=ARS; Records Retention and Disposition for Arizona Counties, www.lib.az.us/records/pdf/County_RD.pdf.

Arkansas: State agencies, Ark. Code Ann. §§ 25-18-601 to -605; county agencies, Ark. Code Ann. §§ 13-4-301 to -308.

California: Government Code § 12236, www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=12001-13000&file=12220-12237; Local Government Records Management Guidelines, www.sos.ca.gov/archives/local-gov-program/pdf/records-management-8.pdf.

Colorado: Colorado Revised Statutes, Title 24, Article 80, www.michie.com/colorado/lpext.dll?f=templates&fn=main-h.htm&cp; Colorado Municipal Records Retention Schedule, www.colorado.gov/dpa/doit/archives/rm/MunicipalRMM/; www.colorado.gov/dpa/doit/archives/rm/MunicipalRMM/Sched7.pdf.

Connecticut: Conn. Gen. Stat. § 11-8. Records management program. Public Records Administrator, www.cga.ct.gov/2009/pub/chap188.htm#Sec11-8.htm; Disposition of Local Government Records, www.cslib.org/publicrecords/prlocalgov.htm.

Delaware: Delaware Public Records Law, 29 Del. Code §§ 501–526, http://delcode.delaware.gov/title29/c005/sc01/index.shtml; General Records Retention Schedules, http://archives.delaware.gov/govsvcs/general_records_retention_schedules/index.shtml.

District of Columbia: D.C. Code, Title 2, Chapter 17, Public Records Management, §§ 2-1701 to 2-1714, http://government.westlaw.com/linkedslice/default.asp?SP=DCC-1000.

Florida:[514] Fla. Stat. § 257.36, Records and information management, www.flsenate.gov/Statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=Ch0257/SEC36.HTM&Title=-%3E2008-%3ECh0257-%3ESection%2036#0257.36; General Records Schedule GS1-SL for State and Local Government Agencies, http://dlis.dos.state.fl.us/barm/genschedules/GS1-SL-2006_RevSept2007.pdf.

Georgia: Georgia Records Act, Ga. Code Ann. § 50-18-90 *et seq*., www.sos.georgia.gov/Archives/who_are_we/rims/best_practices_resources/georgia_records_act.htm; Retention Schedules For Local Government Records, http://sos.georgia.gov/archives/pdf/records_and_information_management_services/rslgr.pdf.

[513] Government Records Division provides records management assistance to state and local agencies, www.archives.state.al.us/officials/rec-center.html.

[514] Services for Records Managers, including records retention scheduling and disposition, http://dlis.dos.state.fl.us/index_RecordsManagers.cfm.

Hawaii: Haw. Rev. Stat., Chapter 92, Public Agency Meetings and Records, § 92-31, Disposition of original record, http://luc.state.hi.us/docs/hrs_92.pdf; § 94-3, Disposal of government records generally, www.capitol.hawaii.gov/hrscurrent/Vol02_Ch0046-0115/HRS0094/HRS_0094-0003.htm; State of Hawaii General Records Schedules, http://hawaii.gov/dags/archives/records-management/GRS%202002%20-%20revised%205-06.pdf; Records Management Process, http://hawaii.gov/dags/archives/Records%20management%20process.pdf.

Idaho: 67-5751 Records Management, www.legislature.idaho.gov/idstat/Title67/T67CH57SECT67-5751.htm, http://adm.idaho.gov/purchasing/RecordsCenter/RecordRetentionBook.pdf.

Illinois: Local Records Act, 50 Ill. Comp. Stat. 205/, www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=699&ChapAct=50%A0ILCS%A0205/&ChapterID=11&ChapterName=LOCAL+GOVERNMENT&ActName=Local+Records+Act.

Indiana: Ind. Code 5-15-5.1, State Commission on Public Records, www.ai.org/legislative/ic/code/title5/ar15/ch5.1.html; Ind. Code 5-15-6, Local Public Records Commissions, www.ai.org/legislative/ic/code/title5/ar15/ch6.html.[515]

Iowa: State Records and Archives, http://www.iowahistory.org/archives/.

Kansas: Kan. Stat. Ann. Chapter 45. —PUBLIC RECORDS, DOCUMENTS AND INFORMATION, Article 4.—PUBLIC RECORDS PRESERVATION [Accessible from www.kslegislature.org/legsrv-statutes/index.do].

Kentucky: State Archives and Records Act, Ky. Rev. Stat. 171.410-171.740, www.lrc.ky.gov/KRS/171-00/CHAPTER.HTM; Local Records Retention Schedules, www.kdla.ky.gov/recmanagement/localschedule.htm.

Louisiana: La. Rev. Stat. Title 44: Public records and recorders, www.legis.state.la.us/lss/lss.asp?folder=118; La. Rev. Stat. § 44:36, Preservation of records, www.legis.state.la.us/lss/lss.asp?doc=99704; La. Rev. Stat. 44:410, www.legis.state.la.us/lss/lss.asp?doc=99731.

Maine: 5 Me. Rev. Stat. Ann. § 95, Powers and duties of State Archivist, www.mainelegislature.org/legis/statutes/5/title5sec95.html; 5 Me. Rev. Stat. Ann. § 95-B, Local government records, www.mainelegislature.org/legis/statutes/5/title5sec95-B.html; Code of Maine Rules, 29 255 Maine State Archives, Chapter 10, Rules for Disposition of Local Government Records, http://www.maine.gov/sos/cec/rules/29/chaps29.htm.

Maryland: Annotated Code of Maryland State Government Article 10, §§ 631–34, www.msa.md.gov/msa/intromsa/html/record_mgmt/pdf/sg_title10_631-634.pdf ; COMAR 14.18.02; County agency records retention and disposition schedules, http://guide.mdsa.net/series.cfm?action=viewDetailedSeries&ID=se53 ; Municipal agency records retention and disposition schedules, http://guide.mdsa.net/series.cfm?action=viewDetailedSeries&ID=se54.

Massachusetts: Mass. Gen. Laws c. 66, § 8, Preservation and destruction of records, books and papers [timeline for keeping state, county, city, and town records], www.mass.gov/legis/laws/mgl/66-8.htm.

Michigan: Mich. Comp. Laws 18.1284–92, Management and Budget Act, Records Management, www.legislature.mi.gov/(S(yfirvcqdnbqsru2k0hguox55))/mileg.aspx?page=getObject&objectName=mcl-Act-431-of-1984; General Schedules for Local Government, www.michigan.gov/hal/0,1607,7-160-17451_18673_31548-56101--,00.html ; Local Government Records Management and Preservation, www.michigan.gov/documents/hal_mhc_rms_Local_RM_Manual_116243_7.pdf.

Minnesota: Minn. Stat. 138.17 Government Records; Administration, www.revisor.leg.state.mn.us/statutes/?id=138.17; Minn. Stat. 138.225, www.revisor.leg.state.mn.us/statutes/?id=138; Prohibition Against Unauthorized Disposal of Records; Penalty; General Records Retention Schedule for Minnesota Cities, www.mcfoa.org/vertical/Sites/%7B067FFB58-E3CD-42BA-9FB1-11EFC7933168%7D/uploads/%7B6ADE9FAA-D990-4057-AF2B-77EB5ED7E3B7%7D.PDF.

[515] For other resources, see www.in.gov/icpr/2771.htm.

Mississippi: Mississippi Code of 1972, Chapter 60, Local Government Records [accessible from http://michie.com/mississippi/lpext.dll?f=templates&fn=main-h.htm&cp=|; Local Government Records Retention Schedule, http://mdah.state.ms.us/recman/schedulemain.php.

Missouri: The State and Local Records Law, Sections 109.200 to 109.310, Missouri Revised Statutes Chapter 109, Public and Business Records, www.moga.mo.gov/STATUTES/C109.HTM; Local Records, Records Schedules, www.sos.mo.gov/archives/localrecs/schedules/.

Montana: Public Records Management, Mont. Code Ann. 2-6-201 through 2-6-214, http://data.opi.mt.gov/bills/MCA_toc/2_6_2.htm; Local Government Records Schedules, http://sos.mt.gov/Records/forms/local/Local_Records_Intro.pdf.

Nebraska: Records Management Act, Neb. Rev. Stat. §§ 84-1201 to 84-1228, www.sos.ne.gov/records-management/records_mgmt_act.html.

Nevada: Nev. Rev. Stat. 239.085 State records: Disposition by Department of Transportation, www.leg.state.nv.us/NRS/NRS-239.html#NRS239Sec085; Nev. Rev. Stat. 239.121-125 Local governmental records, www.leg.state.nv.us/NRS/NRS-239.html#NRS239Sec121; Nev. Rev. Stat. 11.208, Action by contractor against Department of Transportation upon contract for construction, reconstruction, improvement, or maintenance of highway, www.leg.state.nv.us/NRS/NRS-011.html.

New Hampshire: Archives and Records Management Act, N.H. Rev. Stat. Ann. 5:26-5:51, www.gencourt.state.nh.us/rsa/html/NHTOC/NHTOC-I-5.htm; N.H. Rev. Stat. Ann. 33-A:4, Disposition Schedule, www.gencourt.state.nh.us/rsa/html/III/33-A/33-A-3-a.htm.

New Jersey: Public Records, N.J. Rev. Stat. 47:1-1 *et seq*., www.state.nj.us/state/darm/links/statutes.html; N.J.A.C. 15:3 Records Retention, www.state.nj.us/state/darm/links/regulations.html.

New Mexico: Public Records, Section 14-3-1 *et seq*. (accessible from www.conwaygreene.com/nmsu/lpext.dll?f=templates&fn=main-h.htm&2.0); Title 1, General Government Administration, Chapter 19, Local Government Records Retention nd Disposition Schedule (LGRRDS), Part 8, New Mexico Municipalities, www.nmcpr.state.nm.us/nmac/parts/title01/01.019.0008.htm.

New York: Local Government Records Law, Article 57-A, Arts & Cultural Affairs Law, §§ 57-13 through 57-39, www.archives.nysed.gov/a/records/mr_laws_acal57A.pdf; Managing Records, www.archives.nysed.gov/a/records/index.shtml.

North Carolina: North Carolina Archives and History Act, N.C. Gen. Stat. §§ 121[ ]1 *et seq*., www.ncleg.net/EnactedLegislation/Statutes/HTML/ByChapter/Chapter_121.html; 07 NCAC 04M .0101 *et seq*., http://reports.oah.state.nc.us/ncac/title%2007%20-%20cultural%20resources/chapter%2004%20-%20archives%20and%20history/subchapter%20m/subchapter%20m%20rules.pdf.

North Dakota: Records Management Act, N.D. Cent. Code § 54-46-01 *et seq*., www.legis.nd.gov/cencode/t54c46.pdf.

Ohio: Ohio Revised Code, Chapter 149: Documents, Reports, and Records, http://codes.ohio.gov/orc/149; Ohio Rev. Code Ann. § 149.431 Records of governmental or nonprofit organizations receiving governmental funds, http://codes.ohio.gov/orc/149.431.

Oklahoma: Records Management Act, 67 Okla. Stat. §§ 201 through 216, accessible from www.lsb.state.ok.us/osstatuestitle.html.

Oregon: Archiving of Public Records, Or. Rev. Stat. §§ 192.005 to 192.170, www.leg.state.or.us/ors/192.html; Records Management Procedures, Or. Admin. R. §§ 166-030-0005 to 166-030-0070, http://arcweb.sos.state.or.us/rules/OARS_100/OAR_166/166_tofc.html; Oregon State Archives, http://arcweb.sos.state.or.us/banners/legis.htm.

Pennsylvania: 71 Pa. Stat. § 207, Filing and record systems [Title 71, I, Ch. 2, Art. V, accessible from http://government.westlaw.com/linkedslice/default.asp?SP=pac-1000]; 71 Pa. Stat. § 241, The Governor [Tit. 71, I, Ch. 2, Art. VII, accessible from http://government.westlaw.com/linkedslice/default.asp?SP=pac-1000]; Records Management, www.portal.state.pa.us/portal/server.pt/community/records_management/2632.

Rhode Island: R.I. Gen. Laws 38-1 Public Records—Custody and Protection, www.rilin.state.ri.us/Statutes/TITLE38/38-1/INDEX.HTM; R.I. Gen. Laws 38-3 Public Records—Public Records Administration Act, www.rilin.state.ri.us/Statutes/TITLE38/38-3/INDEX.HTM.

South Carolina: S.C. Code Ann. § 30-1-80, www.scstatehouse.gov/code/t30c001.htm.

South Dakota: S.D. Codified Laws 1-27-9 to 1-27-19, Records management programs, http://legis.state.sd.us/statutes/DisplayStatute.aspx?Statute=1-27&Type=Statute; S.D. Codified Laws 1-27-4.1, Format of written contracts, http://legis.state.sd.us/statutes/DisplayStatute.aspx?Type=Statute&Statute=1-27-4.1; South Dakota Municipalities Records Retention and Destruction Schedule, www.state.sd.us/boa/2005%20Municipal%20Manual.pdf ; Records Management, www.state.sd.us/boa/records.htm.

Tennessee: Public Records, Tenn. Code Ann. Title 10, Chapter 7 [Accessible from www.michie.com/tennessee/lpext.dll?f=templates&fn=main-h.htm&cp=tncode]; Rules of Public Records Commission, Chapter 1210-1, www.state.tn.us/sos/rules/1210/1210-01.pdf.

Texas: Preservation and Management of State Records and Other Historical Resources Government Code, Chapter 441, Subchapter L, www.tsl.state.tx.us/slrm/recordspubs/stbull04.html#pres; Section 441.185, Record Retention Schedules, www.tsl.state.tx.us/slrm/recordspubs/stbull04.html#441185.

Utah: Archives and Records Service, 63A Utah Code Chapter 12, www.le.utah.gov/UtahCode/section.jsp?code=63A-12; Retention Schedules, http://archives.utah.gov/recordsmanagement/retention-schedule-menu.html.

Vermont: 3 Vt. Stat. Ann. § 117. Vermont state archives and records administration, www.leg.state.vt.us/statutes/fullsection.cfm?Title=03&Chapter=005&Section=00117; 1 Vt. Stat. Ann. § 317a. Disposition of public records, www.leg.state.vt.us/statutes/fullsection.cfm?Title=01&Chapter=005&Section=00317a.

Virginia: Virginia Public Records Act, Va. Code §§ 42.1-76 to 42.1-90.1, http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+TOC42010000007000000000000.

Washington: Chapter 40.14 Wash. Rev. Code, Preservation and destruction of public records, http://apps.leg.wa.gov/RCW/default.aspx?cite=40.14.

West Virginia: Records Management and Preservation of Essential Records Act, § 5A-8-1 *et seq*., www.legis.state.wv.us/WVCODE/Code.cfm?chap=05a&art=8#08.

Wisconsin: Wis. Stat. § 19.21, Custody and delivery of official property and records, www.legis.state.wi.us/statutes/Stat0019.pdf.

Wyoming: Wy. Stat. §§ 9-2-401 to 9-2-413, http://legisweb.state.wy.us/statutes/titles/Title9/Title9.htm; Wyoming State Archives, Records Management Manual, http://wyoarchives.state.wy.us/RecMan/pdf/RecordsManual.pdf.

APPENDIX E: Sample Nondisclosure Agreements

The Transportation Research Board does not endorse a particular nondisclosure agreement (NDA). Transit agencies should work with their counsel to determine the appropriate format for NDAs intended to protect security information. NDA information is provided here for informational purposes only.

Alaska Department of Transportation NDA for conditional access, http://notes4.state.ak.us/pn/pubnotic.nsf/0/206d3018e91f7b6689256f35005e92f5/$FILE/SSI+non-disclosure+AMHS+Security.pdf.

Port Authority of New York and New Jersey Non-Disclosure and Confidentiality Agreement, http://www.panynj.gov/DoingBusinessWith/contractors/pdfs/MF500107A_nondisc_v1.pdf.

Virginia Department of Transportation CII/SSI Individual Non-Disclosure Agreement, http://vdotforms.vdot.virginia.gov/SearchResults.aspx?filename=CII%20Non-Disclosure%20(Individual)%20V5.PDF.

Virginia Department of Transportation Critical Infrastructure Information (CII), Sensitive Security Information (SSI) Agreement to Establish a Company Representative, http://vdotforms.vdot.virginia.gov/SearchResults.aspx?filename=CII%20Company%20Rep%20V5.pdf.

Department of Homeland Security NDA, www.tsa.gov/assets/pdf/NDA_v2.pdf.

APPENDIX F: Examples of SSI and Non-SSI

The following table is reproduced from FTA's March 2009 *Sensitive Security Information (SSI): Designation, Markings, and Control, Resource Document for Transit Agencies*, page 9, http://transit-safety.volpe.dot.gov/Publications/order/singledoc.asp?docid=968.

Table 1. Examples of SSI and Non-SSI

Might Be SSI	Usually Not SSI
System Design and Operational Information	
Transit system design configurations, including architectural drawings and engineering schematics; critical assets and network topology maps; exposed, unattended, or unprotected assets; critical infrastructure layouts; energy sources; and communications assets and procedures	Environmental, safety, or health information
Installation and design-related operational information concerning critical equipment or components that, if sabotaged, could prevent operation or safe shutdown	Information needed to comply with laws and regulations
Security System Design and Equipment Information	
Records of vulnerabilities or security deficiencies at specified facilities or locations, or within the transit agency in general	Information discernable by casual observation
Records of specific locations and design or operational details of internal security devices, such as sensors, detectors, alarms, and barriers	Budgeting and cost information
Information about the capabilities and limitations of security systems, and methods and times to defeat or degrade equipment, operations, or mitigations	General information about equipment
Security procedures and operations that are of a non-routine nature	Routine administrative data
Information about physical security vulnerabilities and deficiencies, especially if they have not been corrected	Records of past facility and equipment evaluations that do not reveal security-related deficiencies or that reveal deficiencies that have been corrected
Information about intrusion detection, alarm, or assessment equipment, including physical and cybersecurity plans and performance of installed equipment	Installation records for intrusion detection, alarm, or assessment systems
Information about security system design or integration, including heightened-risk operating procedures	Commercial vendor information about security equipment and systems
Data on security personnel assigned to specific transit facilities, including times and locations, where information can not be determined by casual observation	Total number of security personnel assigned to transit system facilities, or the fact that personnel numbers are being increased or decreased
Emergency and Emergency Communications Information	
Some emergency procedures, including heightened-risk operating procedures, contingency plans, and business continuity plans	Fire response and evacuation plans that must be shared with all employees
Records of assessments, drills, or exercises that reveal system or security vulnerabilities	Records of communications equipment used by transit authorities, including emergency management
Ridership Data	
	Information about the number of passengers on individual trains or buses or at a particular time of day

APPENDIX G: Checklist for Assessing Adequacy of Management of Security Information

The following checklist of questions may be useful in assessing the adequacy of the agency's management of security information in its competitive procurement process. Because of the importance of state public records law in assessing the protected status of Restricted Security Information, the checklist also includes issues to look for in researching state law. The parameters of state law may influence counsel's recommendations for structuring procedures to manage security information.

- **Ensuring Agency's Decisional Infrastructure**

  Does the agency's Sensitive Security Information (SSI)/Restricted Security Information policy cover procurement?

  Is the policy applied uniformly?

  Are personnel with significant input into procurement documents adequately trained on the disclosure and management ramifications of including SSI/Restricted Security Information in procurement documents?

  Are personnel who manage procurement documentation adequately trained on the requirements for managing SSI/Restricted Security Information in procurement records?

  Does the agency require that personnel with the requisite expertise, such as legal counsel or records managers, review any public record requests for documents containing SSI/Restricted Security Information?

  Are personnel who manage procurement documents adequately trained on requirements for responding to public records requests for procurement documents containing SSI or Restricted Security Information (procedural requirements under state law; agency procedures for review of public record requests)?

- **Deciding Whether to Include SSI/Restricted Security Information in Procurement Documents**

  Is there a real need to include the information in the documentation?

  If included, can the Restricted Security Information be protected under state law? What are the ramifications of being forced to release the Restricted Security Information?

  What are the contract management ramifications of including the SSI/Restricted Security Information?

- **Protecting SSI/Restricted Security Information Under Contract Management Process**

  Does the agency have the physical and IT security required to adequately secure all contract documents (hard copy and electronic) containing SSI/Restricted Security Information?

  Does the agency adequately manage contractor access to all SSI/Restricted Security Information, including site visits and access to documents needed to perform the contract?

Does the agency adequately manage internal access to all contracts containing SSI/Restricted Security Information?

Do management controls include:

Restricting access to personnel with need to know?

Tracking all copies of documents containing SSI/Restricted Security Information?[516]

Requiring nondisclosure agreements before providing access to SSI/Restricted Security Information?

Requiring background checks that comply with 6 U.S.C. § 1143 before providing access to SSI/Restricted Security Information?

- **State Law Issues to Consider**

Does the state law definition cover electronic records? Has a standard been established for email?

What is the standard for considering contractor records to be public records?

Does state law explicitly address segregation? Do these requirements affect the structure of procurement documents?

Does state law include an exemption for security information? What is the scope of the exemption? Is the exemption mandatory or discretionary? Does the exemption require any specific statement or finding concerning public harm or danger from disclosure of withheld information?

Do state courts look to the Freedom of Information Act in interpreting public disclosure requirements, particularly as applied to security exemptions?

What is the standard of proof in establishing that an exemption applies?

Does state law expressly address contract records?

Have state courts interpreted the applicability of federal security legislation, such as the Critical Infrastructure Information Act of 2002, under state public records law?

[516] Use of a controlled access database to do so could provide a quality control mechanism. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 138, at 20.

ACKNOWLEDGMENTS

This study was performed under the overall guidance of TCRP Project Committee J-5. The Committee is chaired by **Robin M. Reitzes**, San Francisco City Attorney's Office, San Francisco, California. Members are **Rolf G. Asphaug**, Denver Regional Transportation District, Denver, Colorado; **Sheryl King Benford**, Greater Cleveland Regional Transit Authority, Cleveland, Ohio; **Darrell Brown**, Darrell Brown & Associates, New Orleans, Louisiana; **Dennis C. Gardner**, Ogletree, Deakins, Nash, Smoak & Stewart, Houston, Texas; **Clark Jordan-Holmes**, Joyner & Jordan-Holmes, P.A., Tampa, Florida; **Elizabeth M. O'Neill**, Metropolitan Atlanta Rapid Transit Authority, Atlanta, Georgia; **Ellen L. Partridge**, Chicago Transit Authority, Chicago, Illinois; and **James S. Thiel**, Wisconsin Department of Transportation, Madison, Wisconsin. **Rita M. Maristch** provides liaison with the Federal Transit Administration, **James P. LaRusch** serves as liaison with the American Public Transportation Association, and **Gwen Chisholm Smith** represents the TCRP staff.

Transportation Research Board
500 Fifth Street, NW
Washington, DC 20001

ISBN 978-0-309-15483-3
90000
9 780309 154833

Subscriber Categories: Administration and Management • Law • Public Transportation