State of Washington
Joint Legislative Audit and Review Committee (JLARC)

Domestic Security: Exemptions to Public Records Disclosure

Report 04-11

June 16, 2004

Upon request, this document is available in alternative formats for persons with disabilities.

JOINT LEGISLATIVE AUDIT AND REVIEW COMMITTEE
506 16th Avenue SE
PO Box 40910
Olympia, WA 98501-2323
(360) 786-5171
(360) 786-5180 Fax
http://jlarc.leg.wa.gov

The Joint Legislative Audit and Review Committee (JLARC) carries out oversight, review, and evaluation of state-funded programs and activities on behalf of the Legislature and the citizens of Washington State. This joint, bipartisan committee consists of eight senators and eight representatives, equally divided between the two major political parties. Its statutory authority is established in RCW 44.28.

JLARC staff, under the direction of the Committee and the Legislative Auditor, conduct performance audits, program evaluations, sunset reviews, and other policy and fiscal studies. These studies assess the efficiency and effectiveness of agency operations, impacts and outcomes of state programs, and levels of compliance with legislative direction and intent. The Committee makes recommendations to improve state government performance and to correct problems it identifies. The Committee also follows up on these recommendations to determine how they have been implemented. JLARC has, in recent years, received national recognition for a number of its major studies.

DOMESTIC SECURITY: EXEMPTIONS TO PUBLIC RECORDS DISCLOSURE

REPORT 04-11

JUNE 16, 2004

STATE OF WASHINGTON

JOINT LEGISLATIVE AUDIT AND REVIEW COMMITTEE

STUDY TEAM

John Woolley

LEGISLATIVE AUDITOR

Cindi Yates

Copies of Final reports and Digests are available on the JLARC website at:

http://jlarc.leg.wa.gov

or contact

Joint Legislative Audit & Review Committee
506 16th Avenue SE
Olympia, WA 98501-2323
(360) 786-5171
(360) 786-5180 FAX

Overview

In response to the events of September 11, 2001, the Legislature added records related to preventing terrorist attacks and records related to computer and telecommunication networks to the list of exemptions from public disclosure requirements. SSB 6439 (Chapter 335, Laws of 2002) also directed JLARC to review the effect of the law by September 2004 on state agency performance in responding to requests for disclosure of records.

We conclude that the law's impact has been negligible: the volume of requests and denials covered by these exemptions has been very low, resulting in little impact on agencies' workload.

Public Disclosure

The state's public disclosure law **requires** agencies to make available for public inspection and copying all public records, **unless the information is specifically exempted**.

When the Legislature added the domestic security exemptions, the following were specifically exempted from "public inspection and copying" (RCW 42.17.310 (1)(ww) & (ddd)):

- Portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to **criminal terrorist acts**;
- **Vulnerability assessments or deployment plans**, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans;
- Records not subject to public disclosure **under federal laws** that are shared by federal or international agencies;
- Information prepared from **national security briefings** provided to state or local government officials related to domestic preparedness for acts of terrorism; and
- Information regarding the **infrastructure and security of computer and telecommunication networks**.

Terrorist acts are defined as "acts that significantly disrupt the conduct of government or the general civilian population of the state or the United States and that manifest an extreme indifference to human life" (RCW 42.17.310 (1)(ww)).

Impact On State Agency Performance

In assessing the impact of the additional exemptions, JLARC was directed to select a representative sample of up to five state agencies. Based on public testimony on SSB 6439 as it was debated, we reviewed:

- Utilities and Transportation Commission (UTC)
- State Patrol
- Department of Information Systems (DIS)
- Department of Transportation (DOT)
- Military Department

In addition to these five agencies, we spoke with the Attorney General's Office to determine if any appeals on denials have been filed. None have.

To judge the impact of the exemptions, we asked agencies for information on the total number of requests for public records for calendar year 2003. In addition, regardless of their basis, we asked for the number of denials and specifically the number of denials based on the provisions added by SSB 6439 for 2003. We also asked how agencies track requests and their estimate of the exemptions' impact.

	Total Number of Requests in 2003	How Many Denied?	Of the denials, how many based on the new exemptions?	Process for Tracking Requests	Agencies' Estimate of Impact of Added Exemptions
Washington State Patrol	9,914	1,867	0	Database, maintained by each office	Negligible
Department of Transportation	904	42	0	Individual offices track with separate systems	Negligible
Department of Information Services	71	6	3	Head office responsibility, with all requests forwarded to Public Disclosure Officer	Small. While the numbers are low, the exemptions created in SSB 6439 are more complex than other exemptions.
Military Department	24	0	0	Most requests handled by Risk Management Office	Negligible. Agency noted that it has, however, added some complexity to the review process.
Utilities and Transportation Commission	*UTC believes it does not possess documents that are subject to exemption from disclosure under the provisions of SSB 6439. According to the UTC, companies they regulate do not typically file with the Commission the types of records described in SSB 6439.*				

The table shows differences in total numbers of requests for public records disclosure, but only three requests were denied in 2003 based on the new exemptions.

Interestingly, these three denials were only partial. Specific information related to addresses of DIS equipment or disaster recovery plans was redacted (deleted), but the remainder of the request was filled. This is consistent with a memorandum from the Attorney General's Office explaining how the provisions of SSB 6439 should be put in place. The memorandum emphasized the need to redact only the protected information and disclose the remainder of the request (Please see Appendix 3).

A Note on Pipelines and the Utilities and Transportation Commission

Disclosure of pipeline security plans has been an area of concern in Washington State. According to the UTC, the responsibility for the review of these plans has been transferred to the federal Department of Homeland Security. As such, UTC inspectors are not involved and have no documents that might be subject to disclosure.

CONCLUSION

The impact on agencies of these new exemptions to public records disclosure has been negligible. Based on our analysis of information from the five agencies, we conclude that agency performance in responding to requests for information has not been adversely affected.

However, as indicated by both the Department of Information Services and the Military Department, every additional exemption does add a layer of complexity to the review process. These exemption areas could be used more extensively in the future. With a nationwide emphasis on preparing for terrorist attacks, more "information traffic" could be subject to records public disclosure requests in the future.

Cindi Yates
Legislative Auditor

On June 16, 2004, this report was approved for distribution by the Joint Legislative Audit and Review Committee.

Senator Jim Horn
Chair

APPENDIX 1 – SCOPE AND OBJECTIVES

Public Records Disclosure: Review of Impact of Domestic Security Exemptions

PROPOSED SCOPE AND OBJECTIVES

APRIL 21, 2004

STATE OF WASHINGTON

JOINT LEGISLATIVE AUDIT AND REVIEW COMMITTEE

STUDY TEAM

John Woolley

LEGISLATIVE AUDITOR

TOM SYKES

Joint Legislative Audit & Review Committee
506 16th Avenue SE
Olympia, WA 98501-2323
(360) 786-5171
(360) 786-5180 Fax

http://jlarc.leg.wa.gov

MANDATE

In the 2002 Legislative Session, SSB 6439 (Chapter 335, Laws of 2002) established exemptions from public disclosure for records related to preventing terrorist acts and for information related to the infrastructure and security of computer and telecommunication networks. JLARC is to review the impact of these exemptions on agency performance in responding to requests for public records under public disclosure.

BACKGROUND

SSB 6439 added or amended "from public inspection and copying" (RCW 42,17.310) the following exemptions:

- Portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts.
- Deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans.
- Records not subject to public disclosure under federal laws that are shared by federal or international agencies.
- Information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism.
- Information regarding the infrastructure and security of computer and telecommunications networks.

In addition to the exemptions, the bill included definitions of "criminal terrorist act" and "information regarding computer and telecommunications networks."

STUDY SCOPE

As specified by SSB 6439, JLARC is to:

- Review the effect of the bill on state agency performance in responding to requests for disclosure of records.
- Conduct the review by selecting a representative sample of requests, and agency's response to the requests, from up to five state agencies.

STUDY OBJECTIVES

JLARC will determine the effect on agency performance by analyzing the number of requests denied based on the criteria added by SSB 6439. This will be compared to the total number of requests and the total number of denials. We will also provide information on how the selected agencies track requests and denials.

Timeframe for the Study

Report to JLARC in June 2004.

JLARC Staff Contact for the Study

John Woolley (360) 786-5184 woolley_jo@leg.wa.gov

APPENDIX 2 – EXAMPLES OF AGENCY RESPONSE(S)

- Utilities and Transportation Commission
- Department of Information Services

RECEIVED
APR 2 1 2004
JLARC

STATE OF WASHINGTON

WASHINGTON UTILITIES AND TRANSPORTATION COMMISSION

1300 S. Evergreen Park Dr. S.W., P.O. Box 47250 • Olympia, Washington 98504-7250
(360) 664-1160 • TTY (360) 586-8203

April 19, 2004

TO: Tom Sykes, Legislative Auditor

FROM: Carole J. Washburn, Executive Secretary
Utilities and Transportation Commission

RE: JLARC Review of Public Records Disclosure Exemptions

This is the response of the Washington Utilities and Transportation Commission to your request for information about how the Commission has implemented the exemptions added to the Public Records Act by SSB 6439.

Background:

The purpose of the 2002 law was to exempt from disclosure under the Public Records Act records related to efforts to prevent, mitigate or respond to terrorist attacks or records regarding the infrastructure or security of telecommunications and computer networks.

The newly exempted records include:

> "Those portions of records assembled, prepared or maintained to prevent, mitigate or respond to ... terrorist acts ... consisting of:
>
> (i) Specific and unique vulnerability assessments or specific and unique response or deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans; and
>
> (ii) Records not subject to public disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism. "
>
> [RCW 42.17.310(1)(ww)]

And:

> "Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities."
>
> [RCW 42.17.310(1)(aaa)]

Questions:

You asked that we respond to three questions:

1. ***How has the WUTC interpreted the provisions of SSB 6439?***

   To date, the Commission has not had occasion to formally interpret the provisions of SSB 6439 in any adjudication, nor has this issue arisen in any other Commission proceeding.

   The Commission has considered SSB 6439 in the context of responding to public records requests. The Commission has not asserted the exemptions in SSB 6439 because the Commission generally does not possess documents that are subject to exemption from disclosure under that legislation. The primary reason for this is that companies regulated by the Commission typically do not file with the Commission the types of records described in SSB 6439. For example, the Commission does not require regulated companies to file records related to the types of assessments or plans addressed by RCW 42.17.310(1)(ww)(i), nor is the Commission's staff involved in reviewing these materials in the course of their assigned duties.

   Following the September 2001 terrorist attacks, the federal Office of Pipeline Safety (OPS) directed pipeline operators to prepare security plans and identify critical infrastructure. OPS had planned to have pipeline inspectors, including Commission inspectors, review those plans once the operators had prepared them. If this had occurred, such documents would likely have been protected from disclosure under SSB 6439. However, responsibility for review of these plans was subsequently transferred from OPS to the Department of Homeland Security. Consequently, the Commission's pipeline inspectors have not had occasion to either request or review the types of plans covered by this exemption in SSB 6439 for any pipeline operators.

   Similarly, with respect to the exemption in RCW 42.17.310(1)(ww)(ii), for records shared by federal or international agencies, the Commission typically does not receive records from

international agencies. Nor does the Commission receive national security or domestic security information, other than periodic changes in the national alert status. On occasion, the Commission receives information from federal agencies regarding an ongoing incident investigation, such as a pipeline rupture. These records would be exempt under RCW 42.17.310(1)(d), at least until such time as the investigation is completed. If the incident were the result of a terrorist act, some or all of the investigative file could be exempt under SSB 6439. However, this latter issue has not been presented to date.

With respect to the exemption in SSB 6439 for specific types of "information regarding the infrastructure and security of computer and telecommunications networks ..." [RCW 42.17.310(1)(aaa)], the Commission has not received any public records requests for any records that might be exempt under this provision. Telecommunications companies must provide to the Commission contact information for their disaster response and recovery operations (WAC 480-120-414 Emergency operation). While this information would likely be a part of a company's "security and service recovery plan," the Commission has not had reason to decide whether the contact information by itself is exempted by this provision. The emergency operation rule also requires companies to file current plans for emergency operation, including recovery, upon request of the Commission. The Commission has not specifically requested copies of these plans.

2. *What has been its impact on issues related to pipelines?*

Based on our answer to Question 1, SSB 6439 has had no discernable impact on issues related to pipelines. That legislation has not affected the Commission's access to information from pipelines or federal agencies. Nor has it affected the Commission's response to public records requests for pipeline-related records.

3. ***How many requests for public records have been denied by the WUTC based on the law's provisions?***

The Commission has not denied any requests for public records as a result of the exemptions added by SSB 6439, for the reasons explained in our answer to Question 1.

Joint Legislative Audit and Review Committee Review of the Effect of SSB 6439
(Chapter 335, Laws of 2002)

Agency: **Department of Information Services**

Name of Person Completing Questionnaire: **Brian Jensen**

Job Title: **Public Disclosure Officer**

Phone Number: **360.902.2299**

E-Mail: **brianj@dis.wa.gov**

Questions

1. What was the total number of requests for public records made of the agency in calendar year 2003? **Answer: 71**

2. How many of these were denied? **Answer: 6 (DIS presumes that by "denied" JLARC refers to the number of requests for which DIS either provided no records or redacted certain information from one or more of the requested records pursuant to a lawful exemption.)**

3. Of these denials, how many were based on the denial reasons established in SSB 6439? **Answer: 3 (All three were pursuant to RCW 42.17.310(1)(ddd)).**

4. How does the agency track and record requests for public records, denials of those requests, and the reasons for the denials? **Answer: DIS uses an electronic file folder system and a paper filing system to track pending and closed requests.**

   For instance:

   - Do you have a database that tracks requests and denials? **Answer: No.**
   - Is the processing of requests a "head office" responsibility, or are local offices responsible? **Answer: Processing of requests is a "head office" responsibility. All requests for public records are forwarded to the DIS Public Disclosure Officer, located at DIS' main administrative office.**
   - What was the process you used to answer Questions 1 through 3 above? For instance, did you check the database? Review all files in the absence of a database? **Answer: DIS reviewed its electronic and paper files to determine the answers to Questions 1 through 3 above.**

5. Using the following scale, what is your estimate of the **impact of SSB 6439** on the agency's ability to respond to requests for public records? Please explain your answer.

   - High: numbers of denials are such that a substantial increase in workload has taken place and statute-defining exemptions are now more difficult to understand and interpret.
   - Moderate: numbers are such that the agency has experienced a noticeable increase in workload and complexity.

- Small: numbers are such that some increase in workload and complexity has been experienced.
- Negligible: numbers are such that there has been little impact on workload and little added complexity.

Answer: Small. The exemption in RCW 42.17.310(1)(ddd) protecting "[i]nformation regarding the infrastructure and security of computer and telecommunications networks" is particularly complex as compared to the other exemptions in the law. While it applies infrequently, each time this exemption may apply the agency's public disclosure officer usually must meet with agency technical staff to discuss the nature of the information contained in the requested record. In addition, following passage of SSB 6439, DIS legal staff and security staff worked together to understand the scope of the exemption and developed internal document handling and labeling processes.

APPENDIX 3 – ATTORNEY GENERAL'S MEMORANDUM

Christine O. Gregoire
ATTORNEY GENERAL OF WASHINGTON
PO Box 40100 • Olympia WA 98504-0100 • (360) 753-6200

MEMORANDUM

June 4, 2002

TO: Washington State Agencies, Boards and Commissions
Washington State Association of Counties
Association of Washington Cities
Washington Association of Prosecuting Attorneys
Washington Association of Sheriffs and Police Chiefs
Committee on Terrorism
Anti-Terrorism Task Force
Emergency Management Association

FROM: Nancy Krier, Assistant Attorney General
Licensing & Administrative Law Division

Sara Finlay, Assistant Attorney General
Government Operations Division

SUBJECT: **2002 Legislation Related to Public Disclosure, Terrorism and Domestic Preparedness (Laws of 2002, Ch. 335, Effective June 13, 2002)**

INTRODUCTION

This Question and Answer analysis highlights several recent amendments to our state's public disclosure laws that were prompted by the tragic events of September 11, 2001. This analysis focuses on amendments adopted as a result of the passage of Substitute Senate Bill 6439 during the 2002 legislative session.[1] These amendments provide exemptions from public

[1] Four bills were passed in the 2002 legislative session that added a new subsection entitled (aaa) to RCW 42.17.310(1). Pursuant to RCW 1.08.015, the Code Reviser intends to codify those amendments as (aaa) through (ddd), according to their order of signature by the Governor. **(1) Substitute Senate Bill 6439**, Laws of 2002, ch. 335 (effective June 13, 2002) amended the public disclosure laws by modifying the vulnerability assessment/response plan exemption contained in RCW 42.17.310(1)(ww), and adding a new exemption (entitled (aaa)) related to computer and telecommunications infrastructure and security. Subsection (ww), as amended, is the focus of this analysis. **(2)** The amendment in **House Bill 2421**, Laws of 2002, ch. 172 (entitled (aaa), effective June 13, 2002) exempts specific and unique (a) vulnerability assessments or (b) emergency and escape response plans at correctional facilities, if public disclosure would have a substantial likelihood of threatening the security of a correctional facility or any individual's safety. **(3) Substitute Senate Bill 5543**, Laws of 2002, ch. 205 includes an amendment (entitled (aaa), effective March 27, 2002) that exempts information compiled by schools or school districts in the development of their comprehensive safe school plans, to the extent they identify specific vulnerabilities of school districts and each individual school. **(4) Engrossed Substitute House Bill 2453**, Laws of 2002, ch. 224 includes an amendment (entitled (aaa), effective June 13, 2002) regarding the discharge papers of veterans (and is not related to terrorism or domestic preparedness).

disclosure for certain public records related to terrorism and are effective June 13, 2002. This memo discusses the changes in the law and provides practical suggestions for complying with the law. State agency or local government staff is encouraged to consult with our Office, your assigned Assistant Attorney(s) General or legal counsel, as appropriate, when presented with questions about the disclosability of records.

THE LANGUAGE OF THE EXEMPTION(S)

As amended by Laws of 2002, ch. 335 (SSB 6439), RCW 42.17.310(1)(ww) exempts the following from public inspection and copying:

> Those portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts, which are acts that significantly disrupt the conduct of government or of the general civilian population of the state or the United States and that manifest an extreme indifference to human life, the public disclosure of which would have a substantial likelihood of threatening public safety, consisting of:
>
> (i) Specific and unique vulnerability assessments or specific and unique response or deployment plans, including compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans; and
>
> (ii) Records not subject to public disclosure under federal law that are shared by federal or international agencies, and information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism.

Question 1: **How should you construe the new exemptions from disclosure for public records related to terrorism?**

Answer: As you are aware, the courts have recognized that Washington's Public Disclosure Act contains a strong mandate for public disclosure of agency records, and that exemptions from disclosure are to be narrowly construed. The policy of the state of Washington, as expressed in the Act, calls for openness in government in all activities, including domestic preparedness for possible further acts of terrorism. However, when release of those portions of records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts would have a substantial likelihood of threatening public safety, denial of requests for disclosure of such records may be warranted by the new exemptions.

Question 2: **What must an agency demonstrate to qualify for exemption from disclosure of a public record related to terrorism under RCW 42.17.310(1)(ww)?**

Answer: To claim an exemption from public disclosure under the new RCW 42.17.310(1)(ww) as amended during the 2002 legislative session, an agency should be prepared to establish that the portions of public records:

Meet both of two general requirements, as follows:

(1) the records must have been assembled, prepared or maintained to prevent, mitigate, or respond to criminal terrorist acts (which are defined as acts that significantly disrupt the conduct of government or of the general civilian population of the state or the United States and that manifest an extreme indifference to human life); and

(2) public disclosure of the records would have a substantial likelihood of threatening public safety.

Then, the record must fall within one of several types of specific records that are explicitly exempt from disclosure under RCW 42.17.310(1)(ww), as amended, as discussed below.

Question 3: What does the introductory phase "Those portions of records . . ." mean?

Answer: The "terrorism exemption" of SSB 6439 only exempts from disclosure those "portions of records" which meet the specific criteria for exemption. To the extent that such protected information can be deleted from the public record requested, the agency should delete the protected information and disclose a redacted version of the public record (if it is not otherwise exempt from disclosure under another exemption).[2]

Question 4: What is meant by the term "criminal terrorist act"?

Answer: The term is defined by the language of the statute as "acts that significantly disrupt the conduct of government or of the general civilian population of the state or the United States and that manifest an extreme indifference to human life". The exemption is intended to protect documents "assembled, prepared or maintained to prevent, mitigate or respond" to such terrorist acts.

Question 5: What does the term "substantial likelihood of threatening public safety" mean?

Answer: This term is not defined in the statute. Agencies should make their best reasonable judgment, consistent with available information, about the consequences of release of a particular document(s). Agency officials need to be prepared to explain the basis for their determination in the event of court review of the nondisclosure. The burden will be on the agency, not the requesting entity, to show a reviewing court that the record is exempt.

---

[2] However, the redaction requirement does not preclude a vulnerability assessment, response or deployment plan from being withheld in its entirety if that complete record meets the requirements of the "terrorism exemption". Additionally, a record may be protected in its entirety if it is exempt from disclosure pursuant to other laws. See, for example, RCW 42.17.260(1) and RCW 42.17.311.

Question 6: **What are the specific types of records that are exempt under the new "terrorism exemption"?**

Answer: The following portions of public records are exempt from disclosure under RCW 42.17.310(1)(ww) (the "terrorism exemption"), if they are records assembled, prepared, or maintained to prevent, mitigate or respond to criminal terrorist acts and public disclosure would have a substantial likelihood of threatening public safety:

(a) specific and unique vulnerability assessments;
(b) specific and unique response plans;
(c) specific and unique deployment plans;
(d) compiled underlying data collected in preparation of or essential to those vulnerability assessments or response or deployment plans;
(e) records that are not subject to public disclosure under federal law that are shared by federal or international agencies; and
(f) information prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism.

Question 7: **What does the requirement of "specific and unique" mean in relation to vulnerability assessments and response or deployment plans?**

Answer: Although those terms are not defined in RCW 42.17.310(1)(ww),[3] a vulnerability assessment, response or deployment plan should be considered "specific and unique" for purposes of the "terrorism exemption" if it is focused on possible terrorist acts, targets, hazards, system weaknesses or responses and was assembled, prepared or maintained to prevent, mitigate, or respond to criminal terrorist acts.

Question 8: **How do you define "vulnerability assessment," "response," or "deployment" plans?**

Answer: Although those terms are not defined in the statute, the legislative history makes it clear that the Legislature was addressing records assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts in an emergency management planning context. A "vulnerability assessment" is typically part of a hazard or risk analysis that determines risks and consequences. A "response" plan usually is a detailed strategy and preparation for preventing,

[3] Note that the new school safety plan exemption (in SSB 5543) relates to "specific vulnerabilities of school districts and each individual school", and the new correctional facility exemption (in HB 2421) refers to "specific and unique vulnerability assessments or specific and unique emergency and escape response plans".

mitigating, or responding to the hazards identified and addressed in a vulnerability assessment or other analysis of risks. A "deployment" plan generally addresses specific actions to be taken by law enforcement personnel, fire fighters, medical professionals, and others responding to an event.

Question 9: **Can data or inventories of sensitive information be covered by the new "terrorism exemption"?**

Answer: Yes. If the other criteria for coverage by the "terrorism exemption" are met, the (ww) amendments made by SSB 6439 specifically include "compiled underlying data collected in preparation of or essential to the assessments, or to the response or deployment plans". By use of the term "compiled", this section protects information or records that are gathered in preparation of, or essential to, covered assessments, response and vulnerability plans. At the heart of the discussion over this amendment was an understanding that agencies may be, for the first time, bringing together compilations of data that are extremely sensitive in a compiled form. The exemption clearly seeks to protect such information where gathered specifically for preventing, mitigating or responding to terrorist acts.

Question 10: **What types of records are not subject to disclosure under federal law that may be covered by the new "terrorism exemption"?**

Answer: Remember that to qualify for an exemption under RCW 42.17.310(1)(ww)(ii) as records that are exempt under federal law and shared by federal or international agencies, such records must be "assembled, prepared, or maintained to prevent, mitigate, or respond to criminal terrorist acts . . . the public disclosure of which would have a substantial likelihood of threatening public safety". The following are a few examples of records that may not be subject to disclosure under federal law pursuant to the federal Freedom of Information Act (FOIA) at 5 U.S.C. §552(b):

A. Certain national defense or foreign policy records. FOIA Exemption 1 (5 U.S.C. §552(b)(1)) exempts certain matters that are specifically authorized under criteria established by presidential Executive Order to be kept secret in the interest of national defense or foreign policy, and are in fact properly classified pursuant to such Executive Order. For example, Executive Order 12958 (as amended by Executive Order 13142) allows certain information regarding the following matters to be classified by the federal government: military plans, foreign governments or relations, intelligence activities, national security, or vulnerabilities or capabilities of systems or plans relating to national security.[4]

[4] Executive Order 12958 also allows the federal government to classify certain compilations of individually unclassified information; i.e., using what is known as the "mosaic" or "compilation" approach.

B. Certain law enforcement records. FOIA Exemption 7 (5 U.S.C. §552(b)(7)) contains six specific exemptions regarding certain records or information compiled for law enforcement purposes. Generally, law enforcement records can be withheld under FOIA if their disclosure (1) could reasonably be expected to interfere with enforcement proceedings; (2) would deprive a person of a fair trial right; (3) could reasonably be expected to constitute an unwarranted invasion of personal privacy; (4) could reasonably be expected to disclose a confidential source or certain information furnished by a confidential source; (5) would disclose certain techniques, procedures or guidelines for law enforcement investigations or prosecutions; or (6) could reasonably be expected to endanger the life or physical safety of any individual.

C. Other examples of matters which may be interpreted as exempt under federal law include (1) matters specifically exempt from disclosure by other statutes[5]; (2) critical federal infrastructure information and vulnerability assessments (if they are determined to be predominantly internal documents and disclosure would significantly risk the circumvention of agency regulations or statutes or impede the effectiveness of law enforcement activities);[6] and (3) confidential business information submitted to federal agencies by private entities, which may include vulnerability and infrastructure information of private assets.[7]

FOIA has a requirement that records be redacted to protect only those portions of the records that are nondisclosable.[8] You should consult with the federal agency that created or shared the records with your agency to determine what federal exemptions apply, and notify the federal agency if a public disclosure request is made for records that may be exempt under federal law.

---

[5] Examples of other statutes relied upon to exempt matters from disclosure pursuant to FOIA Exemption 3 (5 U.S.C. §552(b)(3)), are the National Security Act of 1947, as amended (50 U.S.C. §404-3(c)(6)), and the Central Intelligence Agency Act of 1949, as amended (50 U.S.C. §403(g)). Each federal agency's FOIA Annual Report (available through www.usdoj.gov/04foia/other_age.htm) includes citations to statutes relied upon in denying disclosure and data as to the type of exemption relied upon.

[6] The federal Department of Justice has encouraged federal agencies to use FOIA Exemption 2 (5 U.S.C. §552(b)(2)) to protect certain vulnerability assessments. (See, for example, U.S. Attorney General memo and DOJ documents available at www.usdoj.gov/oip/foiapost/2001foiapost19.htm.)

[7] FOIA Exemption 4 (5 U.S.C. §552(b)(4)) relates to certain trade secrets and commercial or financial information.

[8] The FOIA redaction requirement provides, in part, that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt. . . ." 5 U.S.C. §552(b).

Question 11: What is protected under the exemption for records "prepared from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism"?

Answer: The Legislature heard testimony that federal officials were reluctant to share sensitive, terrorist-related information with state and local officials because information may be disclosable under state law. While the terms "national security" and "domestic preparedness" are not defined in the statute, this section provides protection to certain records that state and local officials may create as a result of national security briefings, as well as documents provided by federal agencies as part of a briefing of other government officials.

Question 12: What computer and telecommunications records are exempt under the second public disclosure amendment within SSB 6439?

Answer: Although not considered part of the "terrorism exemption" to the public disclosure law, certain records related to computer and telecommunications infrastructure and security are also now exempt (pursuant to Laws of 2002, ch. 335 (SSB 6439) exemption entitled (aaa)), as follows:

> Information regarding the infrastructure and security of computer and telecommunications networks, consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities.

Question 12A: What is the focus of the computer and telecommunications exemption in SSB 6439?

Answer: This section provides that certain computer and telecommunications security information is exempt from public disclosure. The exemption reflects the interest in protecting the computer and telecommunications infrastructure of public agencies by safeguarding certain specified information. The goal in exempting this information is to provide additional protection for the information stored in these systems and prevent the interruption or destruction of the public agency networks, without depriving the public of information regarding government activities that the public has a right to know.

Question 12B: What types of information could be exempt from disclosure pursuant to the computer and telecommunications exemption in SSB 6439?

Answer: This section exempts certain specified public records or portions of records that contain certain

information regarding the infrastructure and security of computer and telecommunications networks; i.e. information consisting of security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, and security test results to the extent that they identify specific system vulnerabilities. The State Department of Information Services interprets this list as including, for example, information specific to employee access to computer and telecommunication network systems (such as user identification and password, PIN#, and digital certificate information), firewall information (such as type of firewall used and how and where firewalls are connected), circuit information, network diagrams, protocols that define a common set of rules that computers use to communicate on a network, how and where virus protection software is used on the network, security plans (as required by the State Information Services Board), plans to recover service after a disaster, and security risk assessments.

Question 12C: **What information would not be exempt from disclosure pursuant to the computer and telecommunications exemption in SSB 6439?**

Answer: This section does not exempt information such as: the type of application processing software used and version of that software (for example Excel or Lotus), maps or the location of computer or telecommunication data centers, or public internet protocol network identification numbers (IP addresses) for agency internet sites.

Question 13: **Are there any oversight provisions of how state agencies handle public disclosure requests for documents related to terrorism?**

Answer: Yes. With respect to the use of the "terrorism exemption" (ww) contained in SSB 6439 and the computer and telecommunications security exemption contained in SSB 6439 (entitled (aaa)), the new legislation requires the Joint Legislative Audit and Review Committee (JLAARC) to review the effect of those two exemptions on state agency performance by reviewing the record requests of five selected state agencies by September 2004.[9]

[9] Section 2 of SSB 6439 provides as follows:

No later than September 1, 2004, the joint legislative audit and review committee shall review the effect of RCW 42.17.310(1)(ww) and (aaa) on state agency performance in responding to requests for disclosure of records under chapter 42.17 RCW. In conducting this review [JLAARC] shall select a representative sample of requests for public disclosure, and the agencies' responses to those requests, from up to five state agencies. The [JLAARC] shall report its findings to the legislature no later than November 30, 2004.

Question 14: Were there public disclosure amendments this session that specifically related to school records?

Answer: Yes. Information compiled by school districts or schools in the development of comprehensive safe school plans, to the extent that they identify specific vulnerabilities of school districts and each individual school, is now exempt pursuant to the Laws of 2002, ch. 205 (SSB 5543) exemption entitled (aaa). (This amendment was not part of what we generally refer to as the "terrorism exemption".) The specific language of this exemption is as follows:

> Information compiled by school districts or schools in the development of their comprehensive safe school plans pursuant to section 2 of this act [Laws of 2002, ch. 205], to the extent that they identify specific vulnerabilities of school districts and each individual school.

Question 15: Were there public disclosure amendments this session that specifically related to correctional facility records?

Answer: Yes. The Laws of 2002, ch. 172 (HB 2421) exemption entitled (aaa) exempts specific and unique vulnerability assessments or specific and unique emergency and escape response plans at adult or juvenile state and local correctional facilities, if disclosure would have a substantial likelihood of threatening a correctional facility's security or an individual's safety. (This amendment was not part of what we generally refer to as the "terrorism exemption".) The specific language of this exemption is as follows:

> Those portions of records containing specific and unique vulnerability assessments or specific and unique emergency and escape response plans at a city, county, or state adult or juvenile correctional facility, the public disclosure of which would have a substantial likelihood of threatening the security of a city, county, or state adult or juvenile correctional facility or any individual's safety.

PRACTICAL SUGGESTIONS

In addition to following standard public disclosure practices, and consulting with legal counsel whenever use of the SSB 6439 exemptions are contemplated, you may want to consider the following suggestions:

A. **Analyze Records Under the SSB 6439 (ww) and (aaa) Amendments**. Agencies should critically analyze and review whether records appropriately should be considered exempt under the revised (ww) or (aaa) exemptions of SSB 6439. Remember that many documents, even those that deal with terrorism, will be

disclosable or disclosable in part. Only those portions of records that fall within the specific standards and listed exemptions of the new law are exempt from disclosure, unless otherwise exempt under other laws.

B. **Clearly Identify Documents Consistent With the Language of the Statute.** If the document you are creating is, in reality, an assessment of particular vulnerabilities to terrorist acts or a plan for responding to a terrorist-related situation or event, or for deploying personnel in such a situation, clearly identify the document as a vulnerability assessment, response plan, or deployment plan.

C. **Label Records.** You may want to label agency records that are subject to the exemptions discussed in this Question & Answer analysis. For example:

If exempt records are shared between your agency and other agencies, label the records accordingly or request that the other agency label the records. The labels should identify that the records are exempt or nondisclosable under a specific state law, or if from a federal agency, under a specific federal law.. (If such records are subsequently claimed as exempt, the source of such information and cited exemption will be important. As discussed herein, you should also notify the agency of origin if records received from it are sought in a public record request. See RCW 42.17.330).

If records are prepared by your agency from national security briefings provided to state or local government officials related to domestic preparedness for acts of terrorism, label the records accordingly. (If such material is subsequently claimed as exempt pursuant to RCW 42.17.310(1)(ww)(ii), the source of such information will be important.)

If records contain information regarding the infrastructure and security of computer and telecommunications networks, label the records accordingly.

Of course, labeling will not affect whether a public record is disclosable under state law. However, labeling could assist public agency staff responding to public records requests, and could assist a court conducting an *in camera* review of the records pursuant to RCW 42.17.340(3).

- A suggested label could read: "All or part of this document is exempt from public disclosure pursuant to RCW 42.17.310(1)(ww) [or such other exemption as appropriate]. Requests for public disclosure of this document, or parts thereof, should be referred immediately to [insert name and number of agency or individual]."

- Depending on the documents, the agency may also want to label them with language such as: "Further distribution of this document is prohibited," "Further distribution of this document is prohibited unless authorized in writing in advance

by [insert name and number of individual]," or "Distribution of this document beyond [insert list of agencies or individuals] is prohibited."

D. **Attach or Reference Compiled Underlying Data.** Consider attaching or referencing compiled underlying data that was assembled in preparation of or essential to vulnerability assessments or response or deployment plans.

E. **Address Records Access Procedures.** Identify who has access to records that may be exempt under the new amendments, and educate them about the exemptions from disclosure. Eliminate unauthorized or unnecessary access by agency personnel, consultants, vendors, etc., to records that may be exempt from disclosure. Consider placing records subject to the "terrorism exemption" in one location with limited access. In some situations it may be appropriate to utilize a sign-out or tracking procedure to control access to exempt documents.

F. **Update Records Management Policies.** In light of the information provided in this memorandum, your agency may want to consider updating its records management policies and procedures.

G. **Address Procedures for Sharing Records.** If your agency sends or receives exempt public records with other public or private entities, your agency should specifically review the suggested procedures in B through F above, including suggestions regarding record identification, labeling, attaching or referencing underlying data, and other records access procedures and management policies.

H. **Maintain Database.** If you are with a state agency, you may want your agency's public record staff to maintain a database to facilitate response to JLAARC should your agency be one of the five chosen for review by September 1, 2004.

I. **Consider Open Public Meetings Procedures.** If it is necessary to discuss an exempt record in a public meeting subject to the Open Public Meetings Act, consult with your agency's AAG(s) or legal counsel regarding the process for such discussion. A governing body subject to the Open Public Meetings Act is authorized to hold an executive session during a regular or special meeting to "consider matters affecting national security". (RCW 42.30.110(1)(a)). There is no case law interpreting this section.

CONCLUSION

The Attorney General's Office hopes this information and analysis is of assistance to you. Thank you.

cc: Attorney General's Office Management Team

APPENDIX 3 – ATTORNEY GENERAL'S MEMORANDUM