NCHRP

REPORT 525

Surface Transportation Security

Volume 5

Guidance for Transportation Agencies on Managing Sensitive Information

TRANSPORTATION RESEARCH BOARD
OF THE NATIONAL ACADEMIES

TRANSPORTATION RESEARCH BOARD EXECUTIVE COMMITTEE 2005 (Membership as of February 2005)

OFFICERS

Chair: *Joseph H. Boardman, Commissioner, New York State DOT*
Vice Chair: *Michael D. Meyer, Professor, School of Civil and Environmental Engineering, Georgia Institute of Technology*
Executive Director: *Robert E. Skinner, Jr., Transportation Research Board*

MEMBERS

MICHAEL W. BEHRENS, *Executive Director, Texas DOT*
LARRY L. BROWN, SR., *Executive Director, Mississippi DOT*
DEBORAH H. BUTLER, *Vice President, Customer Service, Norfolk Southern Corporation and Subsidiaries, Atlanta, GA*
ANNE P. CANBY, *President, Surface Transportation Policy Project, Washington, DC*
JOHN L. CRAIG, *Director, Nebraska Department of Roads*
DOUGLAS G. DUNCAN, *President and CEO, FedEx Freight, Memphis, TN*
NICHOLAS J. GARBER, *Professor of Civil Engineering, University of Virginia, Charlottesville*
ANGELA GITTENS, *Consultant, Miami, FL*
GENEVIEVE GIULIANO, *Director, Metrans Transportation Center, and Professor, School of Policy, Planning, and Development, USC, Los Angeles*
BERNARD S. GROSECLOSE, JR., *President and CEO, South Carolina State Ports Authority*
SUSAN HANSON, *Landry University Professor of Geography, Graduate School of Geography, Clark University*
JAMES R. HERTWIG, *President, CSX Intermodal, Jacksonville, FL*
GLORIA J. JEFF, *Director, Michigan DOT*
ADIB K. KANAFANI, *Cahill Professor of Civil Engineering, University of California, Berkeley*
HERBERT S. LEVINSON, *Principal, Herbert S. Levinson Transportation Consultant, New Haven, CT*
SUE MCNEIL, *Director and Professor, Urban Transportation Center, University of Illinois, Chicago*
MICHAEL MORRIS, *Director of Transportation, North Central Texas Council of Governments*
CAROL A. MURRAY, *Commissioner, New Hampshire DOT*
JOHN E. NJORD, *Executive Director, Utah DOT*
PHILIP A. SHUCET, *Commissioner, Virginia DOT*
MICHAEL S. TOWNES, *President and CEO, Hampton Roads Transit, Hampton, VA*
C. MICHAEL WALTON, *Ernest H. Cockrell Centennial Chair in Engineering, University of Texas, Austin*
LINDA S. WATSON, *Executive Director, LYNX—Central Florida Regional Transportation Authority*

MARION C. BLAKEY, *Federal Aviation Administrator, U.S.DOT* (ex officio)
SAMUEL G. BONASSO, *Acting Administrator, Research and Special Programs Administration, U.S.DOT* (ex officio)
REBECCA M. BREWSTER, *President and COO, American Transportation Research Institute, Smyrna, GA* (ex officio)
GEORGE BUGLIARELLO, *Chancellor, Polytechnic University, and Foreign Secretary, National Academy of Engineering* (ex officio)
THOMAS H. COLLINS (Adm., U.S. Coast Guard), *Commandant, U.S. Coast Guard* (ex officio)
JENNIFER L. DORN, *Federal Transit Administrator, U.S.DOT* (ex officio)
JAMES J. EBERHARDT, *Chief Scientist, Office of FreedomCAR and Vehicle Technologies, U.S. Department of Energy* (ex officio)
EDWARD R. HAMBERGER, *President and CEO, Association of American Railroads* (ex officio)
JOHN C. HORSLEY, *Executive Director, American Association of State Highway and Transportation Officials* (ex officio)
ROBERT D. JAMISON, *Acting Administrator, Federal Railroad Administration, U.S.DOT* (ex officio)
EDWARD JOHNSON, *Director, Applied Science Directorate, National Aeronautics and Space Administration* (ex officio)
RICK KOWALEWSKI, *Deputy Director, Bureau of Transportation Statistics, U.S.DOT* (ex officio)
WILLIAM W. MILLAR, *President, American Public Transportation Association* (ex officio)
MARY E. PETERS, *Federal Highway Administrator, U.S.DOT* (ex officio)
SUZANNE RUDZINSKI, *Director, Transportation and Regional Programs, U.S. Environmental Protection Agency* (ex officio)
JEFFREY W. RUNGE, *National Highway Traffic Safety Administrator, U.S.DOT* (ex officio)
ANNETTE M. SANDBERG, *Federal Motor Carrier Safety Administrator, U.S.DOT* (ex officio)
WILLIAM G. SCHUBERT, *Maritime Administrator, U.S.DOT* (ex officio)
JEFFREY N. SHANE, *Under Secretary for Policy, U.S.DOT* (ex officio)
CARL A. STROCK (Maj. Gen., U.S. Army), *Chief of Engineers and Commanding General, U.S. Army Corps of Engineers* (ex officio)

NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM

Transportation Research Board Executive Committee Subcommittee for NCHRP

JOSEPH H. BOARDMAN, *New York State DOT* (Chair)
JOHN C. HORSLEY, *American Association of State Highway and Transportation Officials*
MICHAEL D. MEYER, *Georgia Institute of Technology*
MARY E. PETERS, *Federal Highway Administration*
ROBERT E. SKINNER, JR., *Transportation Research Board*
MICHAEL S. TOWNES, *Hampton Roads Transit, Hampton, VA*
C. MICHAEL WALTON, *University of Texas, Austin*

NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM

NCHRP REPORT 525

Surface Transportation Security

Volume 5

Guidance for Transportation Agencies on Managing Sensitive Information

TRANSTECH MANAGEMENT, INC.
Washington, D.C.

SUBJECT AREAS
Planning and Administration • Transportation Law • Safety and Human Performance • Public Transit • Rail • Aviation • Freight Transportation • Marine Transportation • Security

Research Sponsored by the American Association of State Highway and Transportation Officials
in Cooperation with the Federal Highway Administration

TRANSPORTATION RESEARCH BOARD

WASHINGTON, D.C.
2005
www.TRB.org

NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM

Systematic, well-designed research provides the most effective approach to the solution of many problems facing highway administrators and engineers. Often, highway problems are of local interest and can best be studied by highway departments individually or in cooperation with their state universities and others. However, the accelerating growth of highway transportation develops increasingly complex problems of wide interest to highway authorities. These problems are best studied through a coordinated program of cooperative research.

In recognition of these needs, the highway administrators of the American Association of State Highway and Transportation Officials initiated in 1962 an objective national highway research program employing modern scientific techniques. This program is supported on a continuing basis by funds from participating member states of the Association and it receives the full cooperation and support of the Federal Highway Administration, United States Department of Transportation.

The Transportation Research Board of the National Academies was requested by the Association to administer the research program because of the Board's recognized objectivity and understanding of modern research practices. The Board is uniquely suited for this purpose as it maintains an extensive committee structure from which authorities on any highway transportation subject may be drawn; it possesses avenues of communications and cooperation with federal, state and local governmental agencies, universities, and industry; its relationship to the National Research Council is an insurance of objectivity; it maintains a full-time research correlation staff of specialists in highway transportation matters to bring the findings of research directly to those who are in a position to use them.

The program is developed on the basis of research needs identified by chief administrators of the highway and transportation departments and by committees of AASHTO. Each year, specific areas of research needs to be included in the program are proposed to the National Research Council and the Board by the American Association of State Highway and Transportation Officials. Research projects to fulfill these needs are defined by the Board, and qualified research agencies are selected from those that have submitted proposals. Administration and surveillance of research contracts are the responsibilities of the National Research Council and the Transportation Research Board.

The needs for highway research are many, and the National Cooperative Highway Research Program can make significant contributions to the solution of highway transportation problems of mutual concern to many responsible groups. The program, however, is intended to complement rather than to substitute for or duplicate other highway research programs.

Note: The Transportation Research Board of the National Academies, the National Research Council, the Federal Highway Administration, the American Association of State Highway and Transportation Officials, and the individual states participating in the National Cooperative Highway Research Program do not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the object of this report.

NCHRP REPORT 525: Volume 5

Project 20-59(14)

ISSN 0077-5614

ISBN 0-309-08803-8

Library of Congress Control Number 2004111186

© 2005 Transportation Research Board

Price $21.00

NOTICE

The project that is the subject of this report was a part of the National Cooperative Highway Research Program conducted by the Transportation Research Board with the approval of the Governing Board of the National Research Council. Such approval reflects the Governing Board's judgment that the program concerned is of national importance and appropriate with respect to both the purposes and resources of the National Research Council.

The members of the technical committee selected to monitor this project and to review this report were chosen for recognized scholarly competence and with due consideration for the balance of disciplines appropriate to the project. The opinions and conclusions expressed or implied are those of the research agency that performed the research, and, while they have been accepted as appropriate by the technical committee, they are not necessarily those of the Transportation Research Board, the National Research Council, the American Association of State Highway and Transportation Officials, or the Federal Highway Administration, U.S. Department of Transportation.

Each report is reviewed and accepted for publication by the technical committee according to procedures established and monitored by the Transportation Research Board Executive Committee and the Governing Board of the National Research Council.

Published reports of the

NATIONAL COOPERATIVE HIGHWAY RESEARCH PROGRAM

are available from:

Transportation Research Board
Business Office
500 Fifth Street, NW
Washington, DC 20001

and can be ordered through the Internet at:

http://www.national-academies.org/trb/bookstore

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. On the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Bruce M. Alberts is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. William A. Wulf is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, on its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both the Academies and the Institute of Medicine. Dr. Bruce M. Alberts and Dr. William A. Wulf are chair and vice chair, respectively, of the National Research Council.

The **Transportation Research Board** is a division of the National Research Council, which serves the National Academy of Sciences and the National Academy of Engineering. The Board's mission is to promote innovation and progress in transportation through research. In an objective and interdisciplinary setting, the Board facilitates the sharing of information on transportation practice and policy by researchers and practitioners; stimulates research and offers research management services that promote technical excellence; provides expert advice on transportation policy and programs; and disseminates research results broadly and encourages their implementation. The Board's varied activities annually engage more than 5,000 engineers, scientists, and other transportation researchers and practitioners from the public and private sectors and academia, all of whom contribute their expertise in the public interest. The program is supported by state transportation departments, federal agencies including the component administrations of the U.S. Department of Transportation, and other organizations and individuals interested in the development of transportation. **www.TRB.org**

www.national-academies.org

COOPERATIVE RESEARCH PROGRAMS STAFF FOR NCHRP REPORT 525

ROBERT J. REILLY, *Director, Cooperative Research Programs*
CRAWFORD F. JENCKS, *Manager, NCHRP*
S. A. PARKER, *Senior Program Officer*
EILEEN P. DELANEY, *Director of Publications*
NATALIE BARNES, *Associate Editor*

NCHRP PROJECT 20-59 PANEL FOR PROJECT 20-59(14)
Field of Special Projects—Area of Security

THOMAS HICKS, *Maryland State Highway Administration* (Chair)
DAVID P. ALBRIGHT, *New Mexico Office of Homeland Security*
JAMES D. COOPER, *FHWA (Retired*)
PAUL GOLDEN, *National Infrastructure Protection Center Liaison Representative*
ANTHONY R. KANE, *AASHTO*
VINCENT P. PEARCE, *FHWA*
RAY L. PURVIS, *Missouri DOT (Retired)*
MARY LOU RALLS, *Texas DOT (Retired)*
TERRY SIMMONDS, *Washington State DOT (Retired)*
STEVEN L. ERNST, *FHWA Liaison Representative*
THEOPHILOS C. GEMELAS, *TSA Liaison Representative*
DAVID S. EKERN, *AASHTO Liaison Representative*
MATTHEW D. RABKIN, *Volpe National Transportation Systems Center Liaison Representative*

AUTHOR ACKNOWLEDGMENTS

This study was requested by AASHTO and conducted as part of National Cooperative Highway Research Program (NCHRP) Project 20-59. Project 20-59 is intended to fund quick response studies on behalf of the AASHTO Special Committee on Transportation Security. The report was prepared by Joe Crossett of TransTech Management, Inc. Project 20-59 is guided by a panel that includes Thomas Hicks, David P. Albright, James D. Cooper, Paul Golden, Anthony R. Kane, Vincent Pearce, Ray L. Purvis, Mary Lou Ralls, and Terry Simmonds. This document was reviewed by David Albright (NMDOT), John Gerner (FHWA), Don Hillis (MODOT), Mike McAllister (VaDOT), Mary Lou Ralls (TxDOT), and Terry Simmonds (WDOT). The project was managed by S. A. Parker, CRP Senior Program Officer.

FOREWORD

By S. A. Parker
Senior Program Officer
Transportation Research Board

This fifth volume of *NCHRP Report 525: Surface Transportation Security* will be of interest to officials responsible for protecting sensitive information about transportation assets; included will be chief executive officers, senior executives, operational and technical managers, law enforcement officers, security personnel, and communications and human-resources staff. Consultants, contractors, and others that work with transportation infrastructure owners will also find this volume useful. The objective of *Volume 5: Guidance for Transportation Agencies on Managing Sensitive Information* is to provide basic information about two primary elements that should be the foundation for any transportation agency's sensitive information policy:

1. How to identify sensitive information that must be protected, and
2. How to control access to sensitive information responsibly.

While this document was written to directly address the concerns of state departments of transportation, it is equally applicable to other public agencies with sensitive information related to transportation facilities or emergency preparedness. TransTech Management, Inc., prepared this volume of *NCHRP Report 525* under NCHRP Project 20-59(14).

Emergencies arising from terrorist threats highlight the need for transportation managers to minimize the vulnerability of travelers, employees, and physical assets through incident prevention, preparedness, mitigation, response, and recovery. Managers seek to reduce the chances that transportation vehicles and facilities will be targets or instruments of terrorist attacks and to be prepared to respond to and recover from such possibilities. By being prepared to respond to terrorism, each transportation agency is simultaneously prepared to respond to natural disasters such as hurricanes, floods, and wildfires, as well as human-caused events such as hazardous materials spills and other incidents.

This is the fifth volume of *NCHRP Report 525: Surface Transportation Security,* a series in which relevant information is assembled into single, concise volumes—each pertaining to a specific security problem and closely related issues. These volumes focus on the concerns that transportation agencies are addressing when developing programs in response to the terrorist attacks of September 11, 2001, and the anthrax attacks that followed. Future volumes of the report will be issued as they are completed.

To develop this volume in a comprehensive manner and to ensure inclusion of significant knowledge, available information was assembled from numerous sources, including a number of state departments of transportation. A topic panel of experts in the subject area was established to guide the researchers in organizing and evaluating the collected data and to review the final document.

This volume was prepared to meet an urgent need for information in this area. It records practices that were acceptable within the limitations of the knowledge avail-

able at the time of its preparation. Work in this area is proceeding swiftly, and readers are encouraged to be on the lookout for the most up-to-date information.

Volumes issued under *NCHRP Report 525: Surface Transportation Security* may be found on the TRB website at http://www4.trb.org/trb/crp.nsf/All+Projects/NCHRP+20-59.

CONTENTS

1 Establishing a Sensitive Information Management Policy, 1

2 Identifying Sensitive Information, 3

3 Controlling Access to Sensitive Information, 5

4 Keys for Success, 10

Appendix A Florida DOT's Exempt Documents and Security System Plan Request Form, A-1

Appendix B Texas DOT's Confidential Safety Information Memorandum, B-1

Appendix C Examples of State Legislation to Exempt Selected Sensitive Transportation-Related Information from State "FOIA" Laws, C-1

1

Establishing a Sensitive Information Management Policy

The threat of terrorist attacks against the United States demands greater vigilance among state departments of transportation (DOTs) over access to sensitive information they produce or control. Most information for which DOTs have responsibility poses no threat to transportation security. In the wrong hands, however, some kinds of information could be dangerously misused by individuals or groups intending to inflict harm on the transportation system, its users, employees, or the general public. This information should be protected from inappropriate intentional disclosure (for example, in response to an external email request from a person without the need to know or by a disgruntled employee) and from unintentional disclosure (for example, when unprotected sensitive information is stolen from a DOT employee).

State DOT personnel are, in general, just beginning to learn how to manage sensitive transportation-related information. They are accustomed to sharing information, such as design documents, freely as part of project management with contractors, other state agencies, or individuals. Important documents are rarely kept in secure locations. Furthermore, state-level "sunshine" laws create an environment in which restrictions on access to information are rare.

Despite frequent misconceptions, state and local governments seeking to protect information they produce or control cannot rely on methods reserved for securing federally controlled sensitive information. (See text box on page 2.) State DOTs must, therefore, develop alternative policies for ensuring sensitive information does not fall into the wrong hands, while maintaining public accountability and ensuring management efficiency. Adequate solutions can generally be achieved without recourse to legislative changes.

All DOTs are encouraged to establish and use comprehensive sensitive information management policies. This guide is intended as a useful starting point for state DOT executives and members of state DOT design, construction, or procurement groups who are considering ways to implement basic sensitive information handling practices. It may also be of interest to security and law enforcement personnel, consultants, contractors, and others working with state DOTs.

This guide provides basic information about two primary elements that should be the foundation for any DOT's sensitive information management policy:

1. How to *identify sensitive information* that must be protected and
2. How to *control access to sensitive information* responsibly.

By establishing appropriate policies in each of these areas, DOTs can improve transportation security, while minimizing administrative burden and maintaining appropriate accountability to the public.

Federal Protection of Sensitive Information

This sidebar explains commonly used federal approaches for protecting information, and why they are not generally applicable to information controlled by state DOTs.

1. Classified (National Security) Information
Information can be classified if it relates to the national defense and foreign relations of the United States and requires protection against unauthorized disclosure. Such information, regardless of its physical form or characteristics, must be owned by, produced by or for, or under the control of the U.S. Government. States cannot classify information. Access to classified documents is tightly controlled.

2. Critical Infrastructure Information
Pursuant to the Critical Infrastructure Information Act of 2002 (CII Act), CII includes private sector information related to physical or computer-based assets that may be voluntarily submitted to the Department of Homeland Security (DHS) with the assurance that the information, if it satisfies the requirements of the CII Act, will be protected from public disclosure. States are not able to protect information under the CII Act.

3. Sensitive Security Information
Sensitive security information (SSI) is sensitive information obtained or developed in the conduct of security activities, including research and development, the unauthorized disclosure of which would be detrimental to transportation safety. The Transportation Security Administration (TSA) has enacted regulation on the safeguarding and disclosure of categories of records and information determined by TSA to be SSI, including vulnerability assessments and emergency response plans. However, other sensitive information, although not official SSI under the regulations, may also warrant no public disclosure.

2
Identifying Sensitive Information

DOTs generate thousands of electronic and paper documents every year. Most information produced by DOTs requires no protection. For example, project-related documents for a simple guardrail installation or road-widening project would likely not require any sort of special management. Agencies should be sensitive to the fact that arbitrary and unnecessary restrictions on non-sensitive information increase bureaucracy and may jeopardize legitimate efforts to protect sensitive information. A subset of DOTs' documents, however, can potentially be misused by someone intending to cause harm to the transportation system, its users, its employees, or the general public. Access to this information should be controlled.

WHAT KINDS OF SENSITIVE INFORMATION DO DOTS HAVE?

For most DOTs, information is likely to be considered sensitive if it is useful for (1) selecting a target for an attack and/or (2) planning and executing an attack. Information commonly found in DOTs that may meet these criteria include the following:

■ **Vulnerability/Countermeasure/Risk Assessment Reports.** These data provide detailed information about the vulnerability of a state's transportation infrastructure to terrorist attack; such data are used in planning for protection against future attacks. Most state DOTs have conducted such assessments in the wake of the terrorist attacks of September 11, 2001; and, as AASHTO publishes further guidance on this topic and the federal government develops new rules, many states are likely to continue preparing new or revised reports.

■ **Emergency Response Plans.** These materials provide detailed information about state DOT protocols for responding to and recovery from a range of disasters, including terrorist attacks. Most DOTs are reviewing and updating their emergency response plans to address terrorism. The plans contain sensitive information that could be used by terrorists in planning attacks that injure emergency responders or disrupt their efforts.

■ **Other Sensitive 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. Such documents are

created and retained for many reasons, including use as emergency reference during the construction and reconstruction of transportation infrastructure. As part of these processes, design 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.

HOW CAN DOTS DETERMINE WHICH INFORMATION TO PROTECT?

To help ensure the information protection efforts they undertake are effective, efficient, and defensible, DOTs should use consistent, objective, and documented procedures for identifying sensitive documents. These procedures should be applicable under all circumstances. Scrutinizing all information based on a general set of questions can be an effective tool for ensuring consistent decision making. States may wish to consider the following questions as they develop their own decision-making tools:

- Could this information be used to aid in selecting a target for an attack, and/or for planning and executing an attack?
- Is this information available from other sources (e.g., via the internet or a simple visual inspection of a facility)?
- Is this information regularly distributed outside the agency?
- Will disclosure of this information create potential for loss of life or economic harm?
- Does this information reveal any security features or vulnerabilities?
- Is this information critical to continuity of operations at the DOT?
- Does the agency keep track of the number of existing copies of the document and the locations of these copies?
- Does this information require special software or other devices to be read and understood? How readily available is the software?
- Can the information be sanitized to remove sensitive information?

Transportation agencies are encouraged to tailor their general list of questions to meet their own needs.

3

Controlling Access to Sensitive Information

Once a decision is made that information is considered sensitive, DOTs should ensure that appropriate information management practices are in place to assure its protection. Individuals or groups seeking sensitive information for inappropriate purposes may try to use official channels, such as a "sunshine" law request to obtain copies; alternatively, they may obtain it by stealing from the desk of a careless employee or through a disgruntled worker. DOTs can guard against these and other scenarios by establishing a straightforward and easy-to-implement set of practices that become an ongoing part of document creation, storage, distribution, use, and destruction.

FIVE STEPS FOR DEVELOPING AN INFORMATION PROTECTION POLICY

Following are five practical steps that should be considered for inclusion in any DOT's sensitive information management policies. Each step should be customized to fit the needs of individual DOTs.

Step 1. Create an Oversight Committee for Setting Sensitive Information Policies

As a first step, DOTs should consider creating an oversight committee that can guide overall development and implementation of sensitive information policies, such as how to identify sensitive information and how to protect it. The committee should include agencywide representation and may also have third-party participation from groups directly affected by policies it establishes (e.g., contractors, law enforcement, and federal agencies). It would be responsible for establishing and documenting procedures, ensuring procedures are adhered to, monitoring their effectiveness, and modifying approaches if necessary. New Mexico DOT, for example, has established a committee that oversees its sensitive information policies.

Step 2. Review and Identify DOT's Sensitive Information

DOTs should review all the information they produce and/or control to determine which sensitive information may require protection. For most agencies, this list will include vulnerability reports, emergency response plans, as well as information related to selected infrastructure or other facilities. As they identify sensitive information, agencies may wish to prioritize it according to its sensitivity relative to other information.

Information should be protected at a level commensurate with the risk posed by its possible misuse.

Step 3. Establish a Single Point of Contact for Managing Sensitive Information

To avoid inadvertent dissemination of sensitive information, state DOTS should promote consistent handling and ensure adequate monitoring of potentially suspicious activities. A single internal point of contact (POC) should have day-to-day responsibility for management of sensitive information issues, including identification of sensitive information, documentation of protocols, and handling of information requests. The POC typically may be located in either the office of general counsel, which is familiar with laws governing the release of DOT documents, or the office responsible for records management, which maintains the DOT's public records.

Step 4. Identify Sensitive Information Handling Protocols

Clear and documented agencywide protocols should be established for handling sensitive information in paper and electronic formats. Protocols may address, but need not be limited to, the following:

- **Information access.** Identification of individuals who have a legitimate need to possess sensitive information. Access to sensitive information should be on a "need to know" basis, with more sensitive information being more tightly restricted.
- **Information marking.** Sensitive information should be conspicuously marked with clear warnings that inform holders about the degree of protection required.
- **Information storage and accountability.** Appropriate custodial responsibilities should be established for storing information and tracking its use. The more sensitive the information, the more secure storage should be. Options may include lock and key storage, tamper evident seals, and removal of electronic information from shared computer networks. When electronic distribution of sensitive information to individuals with the need to know is requested, the information should be sent in a password-protected document (with a separate email or phone number to provide the password).
- **Information requests.** Procedures for evaluating requests for sensitive information should be established and be consistent with state "sunshine" and information disclosure laws. For example, Maine DOT and Kentucky Transportation Cabinet (KTC) require all requests to be submitted in a letter indicating what information is needed; why it is needed; and the name, title, and affiliation of the requestor. Florida DOT (FDOT) requires that requests for information on FDOT structures or the FDOT security system plan must be submitted on an "Exempt Documents and Security System Plan Request Form." Requestors must provide their address and phone number, a reason for the request, and a driver's license or photo identification number. (The FDOT Exempt Documents and Security System Plan Request Form are included in Appendix A.)

Agencies may wish to vary the level of protection accorded to individual documents depending on their sensitivity. Policies should, however, always be consistent in the degree of protection they afford to different types of information.

Step 5. Educate DOT Staff About Sensitive Information

Ultimately, physical protection of sensitive information must be the responsibility of every component and employee of the agency. Education is critical to ensuring they understand and follow established procedures. Texas DOT (TxDOT) has distributed a memo to all its employees detailing protocol on sensitive security information handling. Employees are instructed to contact the TxDOT Office of General Counsel whenever there is an "unusual request for information that may relate to public safety or the security of Texas infrastructure." (A copy of the memo is included in Appendix B.) Washington State DOT (WSDOT) has also distributed a memo to employees that requires suspicious requests to be shared with division managers. If the manager determines it is necessary, the request is forwarded to the WSDOT's Record Services Unit for further review.

HANDLING REQUESTS FOR INFORMATION UNDER STATE "SUNSHINE" LAWS

Agencies are encouraged to consult their legal counsel and review existing state legislation to ensure they are adequately equipped to withhold sensitive information in response to public requests. In most instances, under existing state "sunshine" or public disclosure (information act) laws, DOTs should be able to avoid disclosure of sensitive information. Many states model their sunshine laws after the federal Freedom of Information Act (FOIA), which allows federal agencies to protect sensitive security information from public disclosure by using the statutory exemptions contained in FOIA. Key federal exemptions to FOIA that are also likely to be applicable at the state level are as follows:

■ **Exemption 2.** This exempts from mandatory public disclosure agency records "related solely to the internal personnel rules and practices of an agency."[1] The courts have interpreted this exemption as encompassing two different types of information: (1) routine internal administrative matters, in which the public has little interest, often called "low 2" information and (2) more substantial internal matters, the disclosure of which would risk circumvention of a statute or agency regulation, often called "high 2" information. The underlying concept is that a FOIA disclosure should not benefit persons attempting to violate ("circumvent") the law. Application of the high 2 exemption is particularly useful in protecting vulnerability assessments. These are records in which an agency specifically evaluates its own vulnerability (or that of another entity or installation) to safeguard against possible interference or unlawful action—in effect, "circumvention."

■ **Exemption 5.** There may be circumstances where information can be withheld under Exemption 5, which protects "inter-agency or intra-agency memorandums or letters which would not be available by law to a party . . . in litigation with the agency." This includes predecisional documents whose disclosure would inhibit open and frank discussions among government employees in formulating recommendations for agency action.[2] Under Exemption 5, security analyses and recommendations, as well as related draft letters and memorandum, may be protected from release.

---

[1] *The Freedom of Information Act*, *U.S. Code* 5§552(b)(2).

[2] See, e.g., *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 866 (D.C. Cir. 1980) (importance of protecting documents that reflect "the give-and-take of the consultative process").

Departments of transportation in some states may legally be able to protect some information under broad exemptions found in their sunshine laws. In New York for example, release of information can be restricted if it "endangers the life or safety of any person," and in Illinois information may be withheld if it endangers "the life or physical safety of law enforcement personnel or any other person."

Some DOTs have sought to change sunshine-law language to provide specific exemption from public disclosure for information related to critical infrastructure designs and plans, vulnerability assessments, and emergency response plans. Florida, Maryland, Missouri, Texas, Virginia, and Washington have all added exemptions to their state laws that specifically safeguard critical infrastructure data and legally allow them to deny requests for these documents:

- The State of Florida can exempt from public records "building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure. . . ."[3]
- The State of Maryland can exempt "response procedures or plans prepared to prevent or respond to emergency situations, the disclosure of which would reveal vulnerability assessments, specific tactics, specific emergency procedures, or specific security procedures."[4]
- The State of Missouri can exempt information about "existing or proposed security systems and structural plans of real property owned or leased by a public governmental body, the public disclosure of which would threaten public safety."[5]
- The State of Texas can exempt information if "the information is collected, assembled, or maintained by or for a governmental entity for the purpose of preventing, detecting, responding to, or investigating an act of terrorism or related criminal activity . . ."[6]
- The Commonwealth of Virginia can exempt "plans and information to prevent or respond to terrorist activity, disclosure of which would jeopardize the safety of any person, including (i) critical infrastructure sector or structural components; (ii) vulnerability assessments, operational, procedural, transportation, and tactical planning or training manuals, and staff meeting minutes or other records; and (iii) engineering or architectural records . . ."[7]
- The State of Washington can exempt records that have been maintained to respond to criminal terrorist acts as well as "specific and unique vulnerability assessments or emergency response plans intended to prevent or mitigate criminal terrorist acts . . ."[8]

Appendix C contains copies of the referenced legislation.

Before deciding to seek modifications in state law, DOTs should carefully consider whether such efforts are truly necessary to protect information they control, or whether administrative solutions of the kind described in this guide may be satisfactory.

---

[3] *Florida Statutes* §119.07
[4] *Maryland Code* §10.618
[5] *Missouri Revised Statutes* §610.021
[6] *Texas Statutes* §418.177
[7] *Code of Virginia* §2.2-3705.2
[8] *Washington Revised Code* §42.17.310

HOUSING SENSITIVE INFORMATION AT FEDERAL OR LAW ENFORCEMENT AGENCIES

Agencies should use caution when considering partnering with federal or law agencies to house sensitive information outside the DOT as a means for protection. Such strategies do not offer any greater legal justification for limiting disclosure of DOTs' information, and they may create time-consuming and bureaucratic hurdles to legitimately accessing important information.

4
Keys for Success

Sharing information freely when requested is standard operating procedure for state DOTs—this culture reflects the public's need to access information related to project planning, environmental evaluation, and design. Consequently, many states have not yet developed mechanisms to identify, differentiate, and protect sensitive information from that which should and must be made available for public review. Some documents that once seemed appropriate for public use can now be used for potentially deadly purposes, threatening the lives of DOT employees and the citizens they serve. The following should be noted for success:

- Threats to sensitive information may come in the form of (a) official requests for data or documents, or (b) as disclosure of information by disgruntled employees or theft.
- All state DOTs are encouraged (1) to establish and use comprehensive sensitive information management policies tailored to their needs and (2) to provide periodic training on these policies to all employees.
- To ensure optimal efficiency and effectiveness, information should be protected at a level commensurate with the risk posed by its possible misuse.
- Sensitive information management policies should include (1) approaches for identifying sensitive information and (2) management strategies for controlling access to sensitive information.
- Management policies should provide balance between the need to control access to some information and the role of information sharing in public accountability/bureaucratic efficiency.
- State DOTs should follow consistent, objective, and documented practices that apply to all information.

APPENDIX A

Florida DOT's Exempt Documents and Security System Plan

Request Form

STATE OF FLORIDA DEPARTMENT OF TRANSPORTATION

EXEMPT DOCUMENTS AND SECURITY SYSTEM PLAN REQUEST FORM

PART A: EXEMPT DOCUMENTS

Section 119.07(3), Florida Statutes, provides:

> *119.07 Inspection, examination, and duplication of records; exemptions.--*
> *(3)(ee) Building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary and final formats, which depict the internal layout and structural elements of a building, arena stadium, water treatment facility, or other structure owned or operated by an agency as defined i s.119.011 are exempt from the provisions of subsection (1) and s. 24(a), Art. I of the Stat Constitution. This exemption applies to building plans, blueprints, schematic drawings, an diagrams, including draft, preliminary, and final formats, which depict the internal layout an structural elements of a building, arena, stadium, water treatment facility, or other structure owne or operated by an agency before, on, or after the effective date of this act. Information mad exempt by this paragraph may be disclosed to another governmental entity if disclosure i necessary for the receiving entity to perform its duties and responsibilities; to a licensed architec engineer, or contractor who is performing work on or related to the building, arena, stadium, wate treatment facility, or other structure owned or operated by an agency; or upon a showing of goo cause before a court of competent jurisdiction. The entities or persons receiving such informatio shall maintain the exempt status of the information.*

The Exempt Documents being requested are included in those exempt from public disclosure a provided above. The Exempt Documents being requested relate to work being performed for th Florida Department of Transportation or work related to the Department's structures. Th following information is being provided as a record of this request and resulting distribution of th requested Exempt Documents.

Exempt Documents Request Information
Complete all of the following information:

Entity Requesting Documents: (Check One and Provide Full Name of Entity)

____ **Governmental** _____

____ **Architect** _____

____ **Engineer** _____

____ **Contractor** _____

____ **Other** _____

Entity address and phone number:

Address: _____
_____
_____

Phone: _____-_____-_____

Federal ID of Organization requesting (If applicable): _____

Reason for Request/Intended Use of Exempt Documents:

_____
_____
_____

Exempt Documents requested/provided: (Be specific as to all Exempt Documents provided, and include description, project numbers, FIN, contract numbers, etc., that specifically identify all Exempt Documents provided)

_____
_____
_____

Date Exempt Documents provided: _____

Driver license or photo identification number of person receiving Exempt Documents:

_____
(requestor must provide verification of employment with above entity and verify identity with photo ID)

FDOT employee providing Exempt Documents:

FDOT Office: _____ Employee Name: _____

Signature required for receipt of the above Exempt Documents:

I, personally, and/or as representative of the above entity, fully understand the exempt nature of the Exempt Documents I am receiving and agree to maintain the exempt status of this information in accordance with Florida law.

Name of person receiving above Exempt Documents:

(Printed): _____

Signature: _____ **Date:** _____

PART B: SECURITY SYSTEM PLAN

Section 119.071, Florida Statutes, provides:

> *119.071 General exemptions from inspection or copying of public records. -- A security system plan or portion thereof for:*
> *(1) Any property owned by or leased to the state or any of its political subdivisions; or*
> *(2) Any privately owned or leased property*
>
> *which plan or portion thereof is in the possession of any agency, as defined in s. 119.011, is confidential and exempt from the provisions of s. 119.07(1) and s. 24(a), Art. I of the State Constitution. As used in this section, the term a "security system plan" includes all records, information, photographs, audio and visual presentations, schematic diagrams, surveys, recommendations, or consultations or portions thereof relating directly to the physical security of the facility or revealing security systems; threat assessments conducted by any agency as defined in s. 119.011 or any private entity; threat response plans; emergency evacuation plans; sheltering arrangements; or manuals for security personnel, emergency equipment, or security training. This exemption is remedial in nature and it is the intent of the Legislature that this exemption be applied to security system plans received by an agency before, on, or after the effective date of this section. Information made confidential and exempt by this section may be disclosed by the custodial agency to another state or federal agency to prevent, detect, guard against, respond to, investigate, or manage the consequences of any attempted or actual act of terrorism, or to prosecute those persons who are responsible for such attempts or acts, and the confidential and exempt status of such information shall be retained while in the possession of the receiving agency. This section is subject to the Open Government Sunset Review Act of 1995, in accordance with s. 119.15, and shall stand repealed on October 2, 2006, unless reviewed and saved from repeal through reenactment by the Legislature.*

The Security System Plan being requested is confidential and exempt as provided above. The following information is being provided as a record of this request and resulting distribution of the Security System Plan.

Security System Plan Request Information
Complete all of the following information:

Entity Requesting Security System Plan: (Check One and Provide Full Name of Entity)

____ **State Agency** _____

____ **Federal Agency** _____

Entity address and phone number:

Address: _____
_____
_____

Phone: _____-_____-_____

Federal ID of Organization requesting: _____

Reason for Request/Intended Use of Security System Plan:

_____
_____
_____

Security System Plan requested/provided: (Be specific as to all Security System Plan provided, and include description, project numbers, FIN, contract numbers, etc., that specifically identify Security System Plan provided)

_____
_____
_____

Date Security System Plan provided: _____

Driver license or photo identification number of person receiving Security System Plan:

_____

(requestor must provide verification of employment with above entity and verify identity with photo ID)

FDOT employee providing Security System Plan:

FDOT Office: _____ Employee Name: _____

Signature required for receipt of the above Security System Plan:

I, personally, and/or as representative of the above entity, fully understand the confidential and exempt nature of the Security System Plan I am receiving and agree to maintain the confidential and exempt status of this Security System Plan in accordance with Florida law.

Name of person receiving Security

(Printed): _____

Signature: _____ **Date:** _____

APPENDIX B

Texas DOT's Confidential Safety Information Memorandum

Texas
Department
Of Transportation

M E M O R A N D U M

TO: Administration, District Engineers
Division Directors, and Office Directors

DATE: April 29, 2002

FROM: Michael W. Behrens, P.E.

SUBJECT: Confidential Safety Information

The department has a long record of permitting full public access to our documents whenever possible. This continues to be our goal.

Our responsibility to the public, however, requires that we now increase our awareness of security issues at all levels. No area within the department's responsibility poses a greater danger of catastrophic loss of life than a potential threat to our bridges. The events of the last year have shown us all that the threat is far more real than we could have previously imagined. We cannot now continue to release bridge designs and plans to the public as if that threat did not exist.

Therefore, last month Mary Lou Ralls sent you each an email stating that you should contact the Office of General Counsel whenever you get a request for bridge designs or plans and whenever you get any unusual request for information that may relate to public safety or the security of our infrastructure.

Let me reinforce that. No bridge designs or plans are to be released by anyone in the department to members of the public unless you have first contacted the Office of General Counsel for legal advice about whether the information must be released.

APPENDIX C

Examples of State Legislation to Exempt Selected Sensitive Transportation-Related Information from State "FOIA" Laws

Florida State Statutes

119.07 Inspection and copying of records; photographing public records; fees; exemptions

(1)(a) Every person who has custody of a public record shall permit the record to be inspected and copied by any person desiring to do so, at any reasonable time, under reasonable conditions, and under supervision by the custodian of the public records.

(b) A person who has custody of a public record who asserts that an exemption applies to a part of such record shall redact that portion of the record to which an exemption has been asserted and validly applies, and such person shall produce the remainder of such record for inspection and copying.

(c) If the person who has custody of a public record contends that all or part of the record is exempt from inspection and copying, he or she shall state the basis of the exemption that he or she contends is applicable to the record, including the statutory citation to an exemption created or afforded by statute.

(d) If requested by the person seeking to inspect or copy the record, the custodian of public records shall state in writing and with particularity the reasons for the conclusion that the record is exempt or confidential.

(e) In any civil action in which an exemption to this section is asserted, if the exemption is alleged to exist under or by virtue of paragraph (6)(c), paragraph (6)(d), paragraph (6)(e), paragraph (6)(k), paragraph (6)(l), or paragraph (6)(o), the public record or part thereof in question shall be submitted to the court for an inspection in camera. If an exemption is alleged to exist under or by virtue of paragraph (6)(b), an inspection in camera is discretionary with the court. If the court finds that the asserted exemption is not applicable, it shall order the public record or part thereof in question to be immediately produced for inspection or copying as requested by the person seeking such access.

(f) Even if an assertion is made by the custodian of public records that a requested record is not a public record subject to public inspection or copying under this subsection, the requested record shall, nevertheless, not be disposed of for a period of 30 days after the date on which a written request to inspect or copy the record was served on or otherwise made to the custodian of public records by the person seeking access to the record. If a civil action is instituted within the 30-day period to enforce the provisions of this section with respect to the requested record, the custodian of public records may not dispose of the record except by order of a court of competent jurisdiction after notice to all affected parties.

(g) The absence of a civil action instituted for the purpose stated in paragraph (e) does not relieve the custodian of public records of the duty to maintain the record as a public record if the record is in fact a public record subject to public inspection and copying under this subsection and does not otherwise excuse or exonerate the custodian of public records from any unauthorized or unlawful disposition of such record.

(2)(a) As an additional means of inspecting or copying public records, a custodian of public records may provide access to public records by remote electronic means, provided exempt or confidential information is not disclosed.

(b) The custodian of public records shall provide safeguards to protect the contents of public records from unauthorized remote electronic access or alteration and to prevent the disclosure or modification of those portions of public records which are exempt or confidential from subsection (1) or s. 24, Art. I of the State Constitution.

(c) Unless otherwise required by law, the custodian of public records may charge a fee for remote electronic access, granted under a contractual arrangement with a user, which fee may include the direct and indirect costs of providing such access. Fees for remote electronic access provided to the general public shall be in accordance with the provisions of this section.

(3)(a) Any person shall have the right of access to public records for the purpose of making photographs of the record while such record is in the possession, custody, and control of the custodian of public records.

(b) This subsection applies to the making of photographs in the conventional sense by use of a camera device to capture images of public records but excludes the duplication of microfilm in the possession of the clerk of the circuit court where a copy of the microfilm may be made available by the clerk.

(c) Photographing public records shall be done under the supervision of the custodian of public records, who may adopt and enforce reasonable rules governing the photographing of such records.

(d) Photographing of public records shall be done in the room where the public records are kept. If, in the judgment of the custodian of public records, this is impossible or impracticable, photographing shall be done in another room or place, as nearly adjacent as possible to the room where the public records are kept, to be determined by the custodian of public records. Where provision of another room or place for photographing is required, the expense of providing the same shall be paid by the person desiring to photograph the public record pursuant to paragraph (4)(e).

(4) The custodian of public records shall furnish a copy or a certified copy of the record upon payment of the fee prescribed by law. If a fee is not prescribed by law, the following fees are authorized:

(a)1. Up to 15 cents per one-sided copy for duplicated copies of not more than 14 inches by 8½ inches;

2. No more than an additional 5 cents for each two-sided copy; and

3. For all other copies, the actual cost of duplication of the public record.

(b) The charge for copies of county maps or aerial photographs supplied by county constitutional officers may also include a reasonable charge for the labor and overhead associated with their duplication.

(c) An agency may charge up to $1 per copy for a certified copy of a public record.

(d) If the nature or volume of public records requested to be inspected or copied pursuant to this subsection is such as to require extensive use of information technology resources or extensive clerical or supervisory assistance by personnel of the agency involved, or both, the agency may charge, in addition to the actual cost of duplication, a special service charge, which shall be reasonable and shall be based on the cost incurred for such extensive use of information technology resources or the labor cost of the personnel providing the service that is actually incurred by the agency or attributable to the agency for the clerical and supervisory assistance required, or both.

(e)1. Where provision of another room or place is necessary to photograph public records, the expense of providing the same shall be paid by the person desiring to photograph the public records.

2. The custodian of public records may charge the person making the photographs for supervision services at a rate of compensation to be agreed upon by the person desiring to make the photographs and the custodian of public records. If they fail to agree as to the appropriate charge, the charge shall be determined by the custodian of public records.

(5) When ballots are produced under this section for inspection or examination, no persons other than the supervisor of elections or the supervisor's employees shall touch the ballots. The supervisor of elections shall make a reasonable effort to notify all candidates by telephone or otherwise of the time and place of the inspection or examination. All such candidates, or their representatives, shall be allowed to be present during the inspection or examination.

(6)(a) Examination questions and answer sheets of examinations administered by a governmental agency for the purpose of licensure, certification, or employment are exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution. A person who has taken such an examination shall have the right to review his or her own completed examination.

(b)1. Active criminal intelligence information and active criminal investigative information are exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution.

2. A request of a law enforcement agency to inspect or copy a public record that is in the custody of another agency, the custodian's response to the request, and any information that would identify the public record that was requested by the law enforcement agency or provided by the custodian are exempt from the requirements of subsection (1) and s. 24(a), Art. I of the State Constitution, during the period in which the information constitutes criminal intelligence information or criminal investigative information that is active. This exemption is remedial in nature, and it is the intent of the Legislature that the exemption be applied to requests for information received before, on, or after the effective date of this subparagraph. The law enforcement agency shall give notice to the custodial agency when the criminal

intelligence information or criminal investigative information is no longer active, so that the custodian's response to the request and information that would identify the public record requested are available to the public. This subparagraph is subject to the Open Government Sunset Review Act of 1995 in accordance with s. 119.15 and shall stand repealed October 2, 2007, unless reviewed and saved from repeal through reenactment by the Legislature.

(c) Any information revealing the identity of a confidential informant or a confidential source is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution.

(d) Any information revealing surveillance techniques or procedures or personnel is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution. Any comprehensive inventory of state and local law enforcement resources compiled pursuant to part I, chapter 23, and any comprehensive policies or plans compiled by a criminal justice agency pertaining to the mobilization, deployment, or tactical operations involved in responding to emergencies, as defined in s. 252.34(3), are exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution and unavailable for inspection, except by personnel authorized by a state or local law enforcement agency, the office of the Governor, the Department of Legal Affairs, the Department of Law Enforcement, or the Department of Community Affairs as having an official need for access to the inventory or comprehensive policies or plans.

(e) Any information revealing undercover personnel of any criminal justice agency is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution.

(f)1. Any criminal intelligence information or criminal investigative information including the photograph, name, address, or other fact or information which reveals the identity of the victim of the crime of sexual battery as defined in chapter 794; the identity of the victim of a lewd or lascivious offense committed upon or in the presence of a person less than 16 years of age, as defined in chapter 800; or the identity of the victim of the crime of child abuse as defined by chapter 827 and any criminal intelligence information or criminal investigative information or other criminal record, including those portions of court records and court proceedings, which may reveal the identity of a person who is a victim of any sexual offense, including a sexual offense proscribed in chapter 794, chapter 800, or chapter 827, is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution.

2. In addition to subparagraph 1., any criminal intelligence information or criminal investigative information which is a photograph, videotape, or image of any part of the body of the victim of a sexual offense prohibited under chapter 794, chapter 800, or chapter 827, regardless of whether the photograph, videotape, or image identifies the victim, is confidential and exempt from subsection (1) and s. 24(a), Art. I of the State Constitution. This exemption applies to photographs, videotapes, or images held as criminal intelligence information or criminal investigative information before, on, or after the effective date of the exemption.

(g) Any criminal intelligence information or criminal investigative information which reveals the personal assets of the victim of a crime, other than property stolen or destroyed during the commission of the crime, is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution.

(h) All criminal intelligence and criminal investigative information received by a criminal justice agency prior to January 25, 1979, is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution.

(i)1. The home addresses, telephone numbers, social security numbers, and photographs of active or former law enforcement personnel, including correctional and correctional probation officers, personnel of the Department of Children and Family Services whose duties include the investigation of abuse, neglect, exploitation, fraud, theft, or other criminal activities, personnel of the Department of Health whose duties are to support the investigation of child abuse or neglect, and personnel of the Department of Revenue or local governments whose responsibilities include revenue collection and enforcement or child support enforcement; the home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of such personnel; and the names and locations of schools and day care facilities attended by the children of such personnel are exempt from the provisions of subsection (1). The home addresses, telephone numbers, and photographs of firefighters certified in compliance with s. 633.35; the home addresses, telephone numbers, photographs, and places of employment of the spouses and children of such firefighters; and the names and locations of schools and day care facilities attended by the children of such firefighters are exempt from subsection (1). The home addresses and telephone numbers of justices of the Supreme Court, district court of appeal judges, circuit court judges, and county court judges; the home addresses, telephone numbers, and places of employment of the spouses and children of justices and judges; and the names and locations of schools and day care facilities attended by the children of justices and judges are exempt from the provisions of subsection (1). The home addresses, telephone numbers, social security numbers, and photographs of current or former state attorneys, assistant state attorneys, statewide prosecutors, or assistant statewide prosecutors; the home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of current or former state attorneys, assistant state attorneys, statewide prosecutors, or assistant statewide prosecutors; and the names and locations of schools and day care facilities attended by the children of current or former state attorneys, assistant state attorneys, statewide prosecutors, or assistant statewide prosecutors are exempt from subsection (1) and s. 24(a), Art. I of the State Constitution.

2. The home addresses, telephone numbers, social security numbers, and photographs of current or former human resource, labor relations, or employee relations directors, assistant directors, managers, or assistant managers of any local government agency or water management district whose duties include hiring and firing employees, labor contract negotiation, administration, or other personnel-related duties; the names, home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of such personnel; and the names and locations of schools and day care facilities attended by the children of such personnel are exempt from subsection (1) and s. 24(a), Art. I of the State Constitution. This subparagraph is subject to the Open Government Sunset Review

Act of 1995 in accordance with s. 119.15, and shall stand repealed on October 2, 2006, unless reviewed and saved from repeal through reenactment by the Legislature.

3. The home addresses, telephone numbers, social security numbers, and photographs of current or former United States attorneys and assistant United States attorneys; the home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of current or former United States attorneys and assistant United States attorneys; and the names and locations of schools and day care facilities attended by the children of current or former United States attorneys and assistant United States attorneys are exempt from subsection (1) and s. 24(a), Art. I of the State Constitution. This subparagraph is subject to the Open Government Sunset Review Act of 1995 in accordance with s. 119.15 and shall stand repealed on October 2, 2009, unless reviewed and saved from repeal through reenactment by the Legislature.

4. The home addresses, telephone numbers, social security numbers, and photographs of current or former judges of United States Courts of Appeal, United States district judges, and United States magistrate judges; the home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of current or former judges of United States Courts of Appeal, United States district judges, and United States magistrate judges; and the names and locations of schools and day care facilities attended by the children of current or former judges of United States Courts of Appeal, United States district judges, and United States magistrate judges are exempt from subsection (1) and s. 24(a), Art. I of the State Constitution. This subparagraph is subject to the Open Government Sunset Review Act of 1995 in accordance with s. 119.15, and shall stand repealed on October 2, 2009, unless reviewed and saved from repeal through reenactment by the Legislature.

5. The home addresses, telephone numbers, social security numbers, and photographs of current or former code enforcement officers; the names, home addresses, telephone numbers, social security numbers, photographs, and places of employment of the spouses and children of such persons; and the names and locations of schools and day care facilities attended by the children of such persons are exempt from subsection (1) and s. 24(a), Art. I of the State Constitution. This subparagraph is subject to the Open Government Sunset Review Act of 1995 in accordance with s. 119.15, and shall stand repealed on October 2, 2006, unless reviewed and saved from repeal through reenactment by the Legislature.

6. An agency that is the custodian of the personal information specified in subparagraph 1., subparagraph 2., subparagraph 3., subparagraph 4., or subparagraph 5., and that is not the employer of the officer, employee, justice, judge, or other person specified in subparagraph 1., subparagraph 2., subparagraph 3., subparagraph 4., or subparagraph 5., shall maintain the exempt status of the personal information only if the officer, employee, justice, judge, other person, or employing agency of the designated employee submits a written request for maintenance of the exemption to the custodial agency.

(j) Any information provided to an agency of state government or to an agency of a political subdivision of the state for the purpose of forming ridesharing arrangements, which information reveals the identity of an individual who has provided his or her

name for ridesharing, as defined in s. 341.031, is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution.

(k) Any information revealing the substance of a confession of a person arrested is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution, until such time as the criminal case is finally determined by adjudication, dismissal, or other final disposition.

(l)1. A public record which was prepared by an agency attorney (including an attorney employed or retained by the agency or employed or retained by another public officer or agency to protect or represent the interests of the agency having custody of the record) or prepared at the attorney's express direction, which reflects a mental impression, conclusion, litigation strategy, or legal theory of the attorney or the agency, and which was prepared exclusively for civil or criminal litigation or for adversarial administrative proceedings, or which was prepared in anticipation of imminent civil or criminal litigation or imminent adversarial administrative proceedings, is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution until the conclusion of the litigation or adversarial administrative proceedings. For purposes of capital collateral litigation as set forth in s. 27.7001, the Attorney General's office is entitled to claim this exemption for those public records prepared for direct appeal as well as for all capital collateral litigation after direct appeal until execution of sentence or imposition of a life sentence.

2. This exemption is not waived by the release of such public record to another public employee or officer of the same agency or any person consulted by the agency attorney. When asserting the right to withhold a public record pursuant to this paragraph, the agency shall identify the potential parties to any such criminal or civil litigation or adversarial administrative proceedings. If a court finds that the document or other record has been improperly withheld under this paragraph, the party seeking access to such document or record shall be awarded reasonable attorney's fees and costs in addition to any other remedy ordered by the court.

(m) Sealed bids or proposals received by an agency pursuant to invitations to bid or requests for proposals are exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution until such time as the agency provides notice of a decision or intended decision pursuant to s. 120.57(3)(a) or within 10 days after bid or proposal opening, whichever is earlier.

(n) When an agency of the executive branch of state government seeks to acquire real property by purchase or through the exercise of the power of eminent domain all appraisals, other reports relating to value, offers, and counteroffers must be in writing and are exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution until execution of a valid option contract or a written offer to sell that has been conditionally accepted by the agency, at which time the exemption shall expire. The agency shall not finally accept the offer for a period of 30 days in order to allow public review of the transaction. The agency may give conditional acceptance to any option or offer subject only to final acceptance by the agency after the 30-day review period. If a valid option contract is not executed, or if a written offer to sell is not conditionally accepted by the agency, then the exemption from the provisions of this chapter shall expire at the conclusion of the condemnation litigation of the subject property. An agency of the executive branch may exempt title

information, including names and addresses of property owners whose property is subject to acquisition by purchase or through the exercise of the power of eminent domain, from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution to the same extent as appraisals, other reports relating to value, offers, and counteroffers. For the purpose of this paragraph, "option contract" means an agreement of an agency of the executive branch of state government to purchase real property subject to final agency approval. This paragraph shall have no application to other exemptions from the provisions of subsection (1) which are contained in other provisions of law and shall not be construed to be an express or implied repeal thereof.

(o) Data processing software obtained by an agency under a licensing agreement which prohibits its disclosure and which software is a trade secret, as defined in s. 812.081, and agency-produced data processing software which is sensitive are exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution. The designation of agency-produced software as sensitive shall not prohibit an agency head from sharing or exchanging such software with another public agency.

(p) All complaints and other records in the custody of any unit of local government which relate to a complaint of discrimination relating to race, color, religion, sex, national origin, age, handicap, marital status, sale or rental of housing, the provision of brokerage services, or the financing of housing are exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution until a finding is made relating to probable cause, the investigation of the complaint becomes inactive, or the complaint or other record is made part of the official record of any hearing or court proceeding. This provision shall not affect any function or activity of the Florida Commission on Human Relations. Any state or federal agency which is authorized to have access to such complaints or records by any provision of law shall be granted such access in the furtherance of such agency's statutory duties, notwithstanding the provisions of this section. This paragraph shall not be construed to modify or repeal any special or local act.

(q) All complaints and other records in the custody of any agency in the executive branch of state government which relate to a complaint of discrimination relating to race, color, religion, sex, national origin, age, handicap, or marital status in connection with hiring practices, position classifications, salary, benefits, discipline, discharge, employee performance, evaluation, or other related activities are exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution until a finding is made relating to probable cause, the investigation of the complaint becomes inactive, or the complaint or other record is made part of the official record of any hearing or court proceeding. This provision shall not affect any function or activity of the Florida Commission on Human Relations. Any state or federal agency which is authorized to have access to such complaints or records by any provision of law shall be granted such access in the furtherance of such agency's statutory duties, notwithstanding the provisions of this section.

(r) All records supplied by a telecommunications company, as defined by s. 364.02, to a state or local governmental agency which contain the name, address, and telephone number of subscribers are confidential and exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution.

(s)1. Any document that reveals the identity, home or employment telephone number, home or employment address, or personal assets of the victim of a crime and identifies that person as the victim of a crime, which document is received by any agency that regularly receives information from or concerning the victims of crime, is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution. Any information not otherwise held confidential or exempt from the provisions of subsection (1) which reveals the home or employment telephone number, home or employment address, or personal assets of a person who has been the victim of sexual battery, aggravated child abuse, aggravated stalking, harassment, aggravated battery, or domestic violence is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution, upon written request by the victim, which must include official verification that an applicable crime has occurred. Such information shall cease to be exempt 5 years after the receipt of the written request. Any state or federal agency that is authorized to have access to such documents by any provision of law shall be granted such access in the furtherance of such agency's statutory duties, notwithstanding the provisions of this section.

2.a. Any information in a videotaped statement of a minor who is alleged to be or who is a victim of sexual battery, lewd acts, or other sexual misconduct proscribed in chapter 800 or in s. 794.011, s. 827.071, s. 847.012, s. 847.0125, s. 847.013, s. 847.0133, or s. 847.0145, which reveals that minor's identity, including, but not limited to, the minor's face; the minor's home, school, church, or employment telephone number; the minor's home, school, church, or employment address; the name of the minor's school, church, or place of employment; or the personal assets of the minor; and which identifies that minor as the victim of a crime described in this subparagraph, held by a law enforcement agency, is confidential and exempt from subsection (1) and s. 24(a), Art. I of the State Constitution. Any governmental agency that is authorized to have access to such statements by any provision of law shall be granted such access in the furtherance of the agency's statutory duties, notwithstanding the provisions of this section.

b. A public employee or officer who has access to a videotaped statement of a minor who is alleged to be or who is a victim of sexual battery, lewd acts, or other sexual misconduct proscribed in chapter 800 or in s. 794.011, s. 827.071, s. 847.012, s. 847.0125, s. 847.013, s. 847.0133, or s. 847.0145, may not willfully and knowingly disclose videotaped information that reveals the minor's identity to a person who is not assisting in the investigation or prosecution of the alleged offense or to any person other than the defendant, the defendant's attorney, or a person specified in an order entered by the court having jurisdiction of the alleged offense. A person who violates this provision commits a misdemeanor of the first degree, punishable as provided in s. 775.082 or s. 775.083.

(t) Any financial statement which an agency requires a prospective bidder to submit in order to prequalify for bidding or for responding to a proposal for a road or any other public works project is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution.

(u) Where the alleged victim chooses not to file a complaint and requests that records of the complaint remain confidential, all records relating to an allegation of

employment discrimination are confidential and exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution.

(v) Medical information pertaining to a prospective, current, or former officer or employee of an agency which, if disclosed, would identify that officer or employee is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution. However, such information may be disclosed if the person to whom the information pertains or the person's legal representative provides written permission or pursuant to court order.

(w)1. If certified pursuant to subparagraph 2., an investigatory record of the Chief Inspector General within the Executive Office of the Governor or of the employee designated by an agency head as the agency inspector general under s. 112.3189 is exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution until the registration ceases to be active, or a report detailing the investigation is provided to the Governor or the agency head, or 60 days from the inception of the investigation for which the record was made or received, whichever first occurs. Investigatory records are those records which are related to the investigation of an alleged, specific act or omission or other wrongdoing, with respect to an identifiable person or group of persons, based on information compiled by the Chief Inspector General or by an agency inspector general, as named under the provisions of s. 112.3189, in the course of an investigation. An investigation is active if it is continuing with a reasonable, good faith anticipation of resolution and with reasonable dispatch.

2. The Governor, in the case of the Chief Inspector General, or agency head, in the case of an employee designated as the agency inspector general under s. 112.3189, may certify such investigatory records require an exemption to protect the integrity of the investigation or avoid unwarranted damage to an individual's good name or reputation. The certification shall specify the nature and purpose of the investigation and shall be kept with the exempt records and made public when the records are made public.

3. The provisions of this paragraph do not apply to whistle-blower investigations conducted pursuant to the provisions of ss. 112.3187, 112.3188, 112.3189, and 112.31895.

(x)1. The social security numbers of all current and former agency employees which numbers are contained in agency employment records are exempt from subsection (1) and s. 24(a), Art. I of the State Constitution. As used in this paragraph, the term "agency" means an agency as defined in s. 119.011.

2. An agency that is the custodian of a social security number specified in subparagraph 1. and that is not the employing agency shall maintain the exempt status of the social security number only if the employee or the employing agency of the employee submits a written request for confidentiality to the custodial agency. However, upon a request by a commercial entity as provided in s. 119.0721, the custodial agency shall release the last four digits of the exempt social security number, except that a social security number provided in a lien filed with the Department of State shall be released in its entirety. This subparagraph is subject to

the Open Government Sunset Review Act of 1995 in accordance with s. 119.15 and shall stand repealed on October 2, 2009, unless reviewed and saved from repeal through reenactment by the Legislature.

(y) The audit report of an internal auditor prepared for or on behalf of a unit of local government becomes a public record when the audit becomes final. As used in this paragraph, "unit of local government" means a county, municipality, special district, local agency, authority, consolidated city-county government, or any other local governmental body or public body corporate or politic authorized or created by general or special law. An audit becomes final when the audit report is presented to the unit of local government. Audit workpapers and notes related to such audit report are confidential and exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution until the audit is completed and the audit report becomes final.

(z) Any data, record, or document used directly or solely by a municipally owned utility to prepare and submit a bid relative to the sale, distribution, or use of any service, commodity, or tangible personal property to any customer or prospective customer shall be exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution. This exemption commences when a municipal utility identifies in writing a specific bid to which it intends to respond. This exemption no longer applies when the contract for sale, distribution, or use of the service, commodity, or tangible personal property is executed, a decision is made not to execute such contract, or the project is no longer under active consideration. The exemption in this paragraph includes the bid documents actually furnished in response to the request for bids. However, the exemption for the bid documents submitted no longer applies after the bids are opened by the customer or prospective customer.

(aa) Personal information contained in a motor vehicle record that identifies the subject of that record is exempt from subsection (1) and s. 24(a), Art. I of the State Constitution except as provided in this paragraph. Personal information includes, but is not limited to, the subject's social security number, driver identification number, name, address, telephone number, and medical or disability information. For purposes of this paragraph, personal information does not include information relating to vehicular crashes, driving violations, and driver's status. For purposes of this paragraph, "motor vehicle record" means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by the Department of Highway Safety and Motor Vehicles. Personal information contained in motor vehicle records exempted by this paragraph shall be released by the department for any of the following uses:

1. For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles and dealers by motor vehicle manufacturers; and removal of nonowner records from the original owner records of motor vehicle manufacturers, to carry out the purposes of the Automobile Information Disclosure Act, the Motor Vehicle Information and Cost Saving Act, the National Traffic and Motor Vehicle Safety Act of 1966, the Anti-Car Theft Act of 1992, and the Clean Air Act.

2. For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a federal, state, or local agency in carrying out its functions.

3. For use in connection with matters of motor vehicle or driver safety and theft; motor vehicle emissions; motor vehicle product alterations, recalls, or advisories; performance monitoring of motor vehicles, motor vehicle parts, and dealers; motor vehicle market research activities, including survey research; and removal of nonowner records from the original owner records of motor vehicle manufacturers.

4. For use in the normal course of business by a legitimate business or its agents, employees, or contractors, but only:

a. To verify the accuracy of personal information submitted by the individual to the business or its agents, employees, or contractors; and

b. If such information as so submitted is not correct or is no longer correct, to obtain the correct information, but only for the purposes of preventing fraud by, pursuing legal remedies against, or recovering on a debt or security interest against, the individual.

5. For use in connection with any civil, criminal, administrative, or arbitral proceeding in any court or agency or before any self-regulatory body for:

a. Service of process by any certified process server, special process server, or other person authorized to serve process in this state.

b. Investigation in anticipation of litigation by an attorney licensed to practice law in this state or the agent of the attorney; however, the information may not be used for mass commercial solicitation of clients for litigation against motor vehicle dealers.

c. Investigation by any person in connection with any filed proceeding; however, the information may not be used for mass commercial solicitation of clients for litigation against motor vehicle dealers.

d. Execution or enforcement of judgments and orders.

e. Compliance with an order of any court.

6. For use in research activities and for use in producing statistical reports, so long as the personal information is not published, redisclosed, or used to contact individuals.

7. For use by any insurer or insurance support organization, or by a self-insured entity, or its agents, employees, or contractors, in connection with claims investigation activities, anti-fraud activities, rating, or underwriting.

8. For use in providing notice to the owners of towed or impounded vehicles.

9. For use by any licensed private investigative agency or licensed security service for any purpose permitted under this paragraph. Personal information obtained based

on an exempt driver's record may not be provided to a client who cannot demonstrate a need based on a police report, court order, or a business or personal relationship with the subject of the investigation.

10. For use by an employer or its agent or insurer to obtain or verify information relating to a holder of a commercial driver's license that is required under 49 U.S.C. ss. 31301 et seq.

11. For use in connection with the operation of private toll transportation facilities.

12. For bulk distribution for surveys, marketing, or solicitations when the department has obtained the express consent of the person to whom such personal information pertains.

13. For any use if the requesting person demonstrates that he or she has obtained the written consent of the person who is the subject of the motor vehicle record.

14. For any other use specifically authorized by state law, if such use is related to the operation of a motor vehicle or public safety.

15. For any other use if the person to whom the information pertains has given express consent on a form prescribed by the department. Such consent shall remain in effect until it is revoked by the person on a form prescribed by the department.

The restrictions on disclosure of personal information provided by this paragraph shall not in any way affect the use of organ donation information on individual driver licenses nor affect the administration of organ donation initiatives in this state. Personal information exempted from public disclosure according to this paragraph may be disclosed by the Department of Highway Safety and Motor Vehicles to an individual, firm, corporation, or similar business entity whose primary business interest is to resell or redisclose the personal information to persons who are authorized to receive such information. Prior to the department's disclosure of personal information, such individual, firm, corporation, or similar business entity must first enter into a contract with the department regarding the care, custody, and control of the personal information to ensure compliance with the federal Driver's Privacy Protection Act of 1994 and applicable state laws. An authorized recipient of personal information contained in a motor vehicle record, except a recipient under subparagraph 12., may contract with the Department of Highway Safety and Motor Vehicles to resell or redisclose the information for any use permitted under this paragraph. However, only authorized recipients of personal information under subparagraph 12. may resell or redisclose personal information pursuant to subparagraph 12. Any authorized recipient who resells or rediscloses personal information shall maintain, for a period of 5 years, records identifying each person or entity that receives the personal information and the permitted purpose for which it will be used. Such records shall be made available for inspection upon request by the department. The department shall adopt rules to carry out the purposes of this paragraph and the federal Driver's Privacy Protection Act of 1994, 18 U.S.C. ss. 2721 et seq. Rules adopted by the department shall provide for the payment of applicable fees and, prior to the disclosure of personal information pursuant to this paragraph, shall require the meeting of conditions by the requesting person for the purposes of obtaining reasonable assurance concerning the identity of such

requesting person, and, to the extent required, assurance that the use will be only as authorized or that the consent of the person who is the subject of the personal information has been obtained. Such conditions may include, but need not be limited to, the making and filing of a written application in such form and containing such information and certification requirements as the department requires.

(bb) Medical history records and information related to health or property insurance provided to the Department of Community Affairs, the Florida Housing Finance Corporation, a county, a municipality, or a local housing finance agency by an applicant for or a participant in a federal, state, or local housing assistance program are confidential and exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution. Governmental entities or their agents shall have access to such confidential and exempt records and information for the purpose of auditing federal, state, or local housing programs or housing assistance programs. Such confidential and exempt records and information may be used in any administrative or judicial proceeding, provided such records are kept confidential and exempt unless otherwise ordered by a court.

(cc) All personal identifying information; bank account numbers; and debit, charge, and credit card numbers contained in records relating to an individual's personal health or eligibility for health-related services made or received by the Department of Health or its service providers are confidential and exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution, except as otherwise provided in this paragraph. Information made confidential and exempt by this paragraph shall be disclosed:

1. With the express written consent of the individual or the individual's legally authorized representative.

2. In a medical emergency, but only to the extent necessary to protect the health or life of the individual.

3. By court order upon a showing of good cause.

4. To a health research entity, if the entity seeks the records or data pursuant to a research protocol approved by the department, maintains the records or data in accordance with the approved protocol, and enters into a purchase and data-use agreement with the department, the fee provisions of which are consistent with subsection (4). The department may deny a request for records or data if the protocol provides for intrusive follow-back contacts, has not been approved by a human studies institutional review board, does not plan for the destruction of confidential records after the research is concluded, is administratively burdensome, or does not have scientific merit. The agreement must restrict the release of any information, which would permit the identification of persons, limit the use of records or data to the approved research protocol, and prohibit any other use of the records or data. Copies of records or data issued pursuant to this subparagraph remain the property of the department.

This paragraph is subject to the Open Government Sunset Review Act of 1995, in accordance with s. 119.15, and shall stand repealed on October 2, 2006, unless reviewed and saved from repeal through reenactment by the Legislature.

(dd) Bank account numbers and debit, charge, and credit card numbers held by an agency are exempt from subsection (1) and s. 24(a), Art. I of the State Constitution. This exemption applies to bank account numbers and debit, charge, and credit card numbers held by an agency before, on, or after the effective date of this exemption. This paragraph is subject to the Open Government Sunset Review Act of 1995 in accordance with s. 119.15, and shall stand repealed on October 2, 2007, unless reviewed and saved from repeal through reenactment by the Legislature.

(ee) Building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure owned or operated by an agency as defined in s. 119.011 are exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution. This exemption applies to building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout and structural elements of a building, arena, stadium, water treatment facility, or other structure owned or operated by an agency before, on, or after the effective date of this act. Information made exempt by this paragraph may be disclosed to another governmental entity if disclosure is necessary for the receiving entity to perform its duties and responsibilities; 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; or upon a showing of good cause before a court of competent jurisdiction. The entities or persons receiving such information shall maintain the exempt status of the information. This paragraph is subject to the Open Government Sunset Review Act of 1995 in accordance with s. 119.15, and shall stand repealed on October 2, 2007, unless reviewed and reenacted by the Legislature.

[3](ff) Building plans, blueprints, schematic drawings, and diagrams, including draft, preliminary, and final formats, which depict the internal layout or structural elements of an attractions and recreation facility, entertainment or resort complex, industrial complex, retail and service development, office development, or hotel or motel development, which documents are held by an agency as defined in s. 119.011, are exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution. This exemption applies to any such documents held either permanently or temporarily by an agency before or after the effective date of this act. Information made exempt by this paragraph may be disclosed to another governmental entity if disclosure is necessary for the receiving entity to perform its duties and responsibilities; to the owner or owners of the structure in question or the owner's legal representative; or upon a showing of good cause before a court of competent jurisdiction. As used in this paragraph, the term:

1. "Attractions and recreation facility" means any sports, entertainment, amusement, or recreation facility, including, but not limited to, a sports arena, stadium, racetrack, tourist attraction, amusement park, or pari-mutuel facility that:

a. For single-performance facilities:

(I) Provides single-performance facilities; or

(II) Provides more than 10,000 permanent seats for spectators.

b. For serial-performance facilities:

(I) Provides parking spaces for more than 1,000 motor vehicles; or

(II) Provides more than 4,000 permanent seats for spectators.

2. “Entertainment or resort complex” means a theme park comprised of at least 25 acres of land with permanent exhibitions and a variety of recreational activities, which has at least 1 million visitors annually who pay admission fees thereto, together with any lodging, dining, and recreational facilities located adjacent to, contiguous to, or in close proximity to the theme park, as long as the owners or operators of the theme park, or a parent or related company or subsidiary thereof, has an equity interest in the lodging, dining, or recreational facilities or is in privity therewith. Close proximity includes an area within a 5-mile radius of the theme park complex.

3. “Industrial complex” means any industrial, manufacturing, processing, distribution, warehousing, or wholesale facility or plant, as well as accessory uses and structures, under common ownership which:

a. Provides onsite parking for more than 250 motor vehicles;

b. Encompasses 500,000 square feet or more of gross floor area; or

c. Occupies a site of 100 acres or more, but excluding wholesale facilities or plants that primarily serve or deal onsite with the general public.

4. “Retail and service development” means any retail, service, or wholesale business establishment or group of establishments which deals primarily with the general public onsite and is operated under one common property ownership, development plan, or management that:

a. Encompasses more than 400,000 square feet of gross floor area; or

b. Provides parking spaces for more than 2,500 motor vehicles.

5. “Office development” means any office building or park operated under common ownership, development plan, or management that encompasses 300,000 or more square feet of gross floor area.

6. “Hotel or motel development” means any hotel or motel development that accommodates 350 or more units.

This exemption does not apply to comprehensive plans or site plans, or amendments thereto, which are submitted for approval or which have been approved under local land development regulations, local zoning regulations, or development-of-regional-impact review.

(gg)1. Until January 1, 2006, if a social security number, made confidential and exempt pursuant to s. 119.0721, created pursuant to s. 1, ch. 2002-256, passed during the 2002 regular legislative session, or a complete bank account, debit, charge, or credit card number made exempt pursuant to paragraph (dd), created pursuant to s. 1, ch. 2002-257, passed during the 2002 regular legislative session, is or has been included in a court file, such number may be included as part of the court record available for public inspection and copying unless redaction is requested by the holder of such number, or by the holder's attorney or legal guardian, in a signed, legibly written request specifying the case name, case number, document heading, and page number. The request must be delivered by mail, facsimile, electronic transmission, or in person to the clerk of the circuit court. The clerk of the circuit court does not have a duty to inquire beyond the written request to verify the identity of a person requesting redaction. A fee may not be charged for the redaction of a social security number or a bank account, debit, charge, or credit card number pursuant to such request.

2. Any person who prepares or files a document to be recorded in the official records by the county recorder as provided in chapter 28 may not include a person's social security number or complete bank account, debit, charge, or credit card number in that document unless otherwise expressly required by law. Until January 1, 2006, if a social security number or a complete bank account, debit, charge or credit card number is or has been included in a document presented to the county recorder for recording in the official records of the county, such number may be made available as part of the official record available for public inspection and copying. Any person, or his or her attorney or legal guardian, may request that a county recorder remove from an image or copy of an official record placed on a county recorder's publicly available Internet website, or a publicly available Internet website used by a county recorder to display public records outside the office or otherwise made electronically available outside the county recorder's office to the general public, his or her social security number or complete account, debit, charge, or credit card number contained in that official record. Such request must be legibly written, signed by the requester, and delivered by mail, facsimile, electronic transmission, or in person to the county recorder. The request must specify the identification page number of the document that contains the number to be redacted. The county recorder does not have a duty to inquire beyond the written request to verify the identity of a person requesting redaction. A fee may not be charged for redacting such numbers.

3. Upon the effective date of this act, subsections (3) and (4) of s. 119.0721, do not apply to the clerks of the court or the county recorder with respect to circuit court records and official records.

4. On January 1, 2006, and thereafter, the clerk of the circuit court and the county recorder must keep complete bank account, debit, charge, and credit card numbers exempt as provided for in paragraph (dd), and must keep social security numbers confidential and exempt as provided for in s. 119.0721, without any person having to request redaction.

(hh) All personal identifying information contained in records relating to a person's health held by local governmental entities or their service providers for the purpose of determining eligibility for paratransit services under Title II of the Americans with

Disabilities Act or eligibility for the transportation disadvantaged program as provided in part I of chapter 427 is confidential and exempt from the provisions of subsection (1) and s. 24(a), Art. I of the State Constitution, except as otherwise provided herein. This exemption applies to personal identifying information contained in such records held by local governmental entities or their service providers before, on, or after the effective date of this exemption. Information made confidential and exempt by this paragraph shall be disclosed:

1. With the express written consent of the individual or the individual's legally authorized representative;

2. In a medical emergency, but only to the extent necessary to protect the health or life of the individual;

3. By court order upon a showing of good cause; or

4. For the purpose of determining eligibility for paratransit services if the individual or the individual's legally authorized representative has filed an appeal or petition before an administrative body of a local government or a court.

(ii) Any videotape or video signal that, under an agreement with an agency, is produced, made, or received by, or is in the custody of, a federally licensed radio or television station or its agent is exempt from this chapter.

(jj) Any information that would identify or help to locate a child who participates in government-sponsored recreation programs or camps or the parents or guardians of such child, including, but not limited to, the name, home address, telephone number, social security number, or photograph of the child; the names and locations of schools attended by such child; and the names, home addresses, and social security numbers of parents or guardians of such child is exempt from subsection (1) and s. 24(a), Art. I of the State Constitution. Information made exempt pursuant to this paragraph may be disclosed by court order upon a showing of good cause. This exemption applies to records held before, on, or after the effective date of this exemption.

(7) Nothing in this section shall be construed to exempt from subsection (1) a public record which was made a part of a court file and which is not specifically closed by order of court, except as provided in paragraphs (c), (d), (e), (k), (l), and (o) of subsection (6) and except information or records which may reveal the identity of a person who is a victim of a sexual offense as provided in paragraph (f) of subsection (6).

(8) Nothing in subsection (6) or any other general or special law shall limit the access of the Auditor General, the Office of Program Policy Analysis and Government Accountability, or any state, county, municipal, university, board of community college, school district, or special district internal auditor to public records when such person states in writing that such records are needed for a properly authorized audit, examination, or investigation. Such person shall maintain the exempt or confidential status of a public record that is exempt or confidential from the provisions of subsection (1) and shall be subject to the same penalties as the custodian of that record for public disclosure of such record.

(9) An exemption from this section does not imply an exemption from s. 286.011. The exemption from s. 286.011 must be expressly provided.

(10) The provisions of this section are not intended to expand or limit the provisions of Rule 3.220, Florida Rules of Criminal Procedure, regarding the right and extent of discovery by the state or by a defendant in a criminal prosecution or in collateral postconviction proceedings. This section may not be used by any inmate as the basis for failing to timely litigate any postconviction action.

Maryland Code

State Government, Title 10: Governmental Procedures

§ 10-618. Permissible denials

(a) *In general.*—Unless otherwise provided by law, if a custodian believes that inspection of a part of a public record by the applicant would be contrary to the public interest, the custodian may deny inspection by the applicant of that part, as provided in this section.

(b) *Interagency and intra-agency documents.*—A custodian may deny inspection of any part of an interagency or intra-agency letter or memorandum that would not be available by law to a private party in litigation with the unit.

(c) *Examinations.*—(1) Subject to paragraph (2) of this subsection, a custodian may deny inspection of test questions, scoring keys, and other examination information that relates to the administration of licenses, employment, or academic matters.(2) After a written promotional examination has been given and graded, a custodian shall permit a person in interest to inspect the examination and the results of the examination, but may not permit the person in interest to copy or otherwise to reproduce the examination.

(d) *Research projects.*—(1) Subject to paragraph (2) of this subsection, a custodian may deny inspection of a public record that contains the specific details of a research project that an institution of the State or of a political subdivision is conducting.(2) A custodian may not deny inspection of the part of a public record that gives only the name, title, expenditures, and date when the final project summary will be available.

(e) *Real property.*—(1) Subject to paragraph (2) of this subsection or other law, until the State or a political subdivision acquires title to property, a custodian may deny inspection of a public record that contains a real estate appraisal of the property.(2) A custodian may not deny inspection to the owner of the property.

(f) *Investigations.*—(1) Subject to paragraph (2) of this subsection, a custodian may deny inspection of:(i) records of investigations conducted by the Attorney General, a State's Attorney, a city or county attorney, a police department, or a sheriff;(ii) an investigatory file compiled for any other law enforcement, judicial, correctional, or prosecution purpose; or (iii) records that contain intelligence information or security procedures of the Attorney General, a State's Attorney, a city or county attorney, a police department, a State or local correctional facility, or a sheriff.(2) A custodian may deny inspection by a person in interest only to the extent that the inspection would:(i) interfere with a valid and proper law enforcement proceeding;(ii) deprive another person of a right to a fair trial or an impartial adjudication;(iii) constitute an unwarranted invasion of personal privacy;(iv) disclose the identity of a confidential source;(v) disclose an investigative technique or procedure;(vi) prejudice an investigation; or(vii) endanger the life or physical safety of an individual.

(g) *Site-specific location of certain plants, animals or property.*—(1) A custodian may deny inspection of a public record that contains information concerning the site-specific location of an endangered or threatened species of plant or animal, a species of plant or animal in need of conservation, a cave, or a historic property as defined in

Article 83B, § 5-601 (k) of the Code.(2) A custodian may not deny inspection of a public record described in paragraph (1) of this subsection if requested by:(i) the owner of the land upon which the resource is located; or(ii) any entity that could take the land through the right of eminent domain.

(h) *Inventions owned by State public institutions of higher education.*—(1) Subject to paragraph (2) of this subsection, a custodian may deny inspection of that part of a public record that contains information disclosing or relating to an invention owned in whole or in part by a State public institution of higher education for 4 years to permit the institution to evaluate whether to patent or market the invention and pursue economic development and licensing opportunities related to the invention.(2) A custodian may not deny inspection of a part of a public record described in paragraph (1) of this subsection if:(i) the information disclosing or relating to an invention has been published or disseminated by the inventors in the course of their academic activities or disclosed in a published patent;(ii) the invention referred to in that part of the record has been licensed by the institution for at least 4 years; or(iii) 4 years have elapsed from the date of the written disclosure of the invention to the institution.

(i) *Trade secrets, confidential commercial information, confidential financial information of the Maryland Technology Development Corporation.*—A custodian may deny inspection of that part of a public record that contains information disclosing or relating to a trade secret, confidential commercial information, or confidential financial information owned in whole or in part by the Maryland Technology Development Corporation.

(j) *Denial of inspection.*—(1) Subject to paragraphs (2), (3), and (4) of this subsection, a custodian may deny inspection of:(i) response procedures or plans prepared to prevent or respond to emergency situations, the disclosure of which would reveal vulnerability assessments, specific tactics, specific emergency procedures, or specific security procedures;(ii) 1. building plans, blueprints, schematic drawings, diagrams, operational manuals, or other records of airports and other mass transit facilities, bridges, tunnels, emergency response facilities or structures, buildings where hazardous materials are stored, arenas, stadiums, waste and water systems, and any other building, structure, or facility, 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; or 2. records of any other building, structure, or facility, the disclosure of which would reveal the building's, structure's, or facility's life, safety, and support systems, surveillance techniques, alarm or security systems or technologies, operational and evacuation plans or protocols, or personnel deployments; or (iii) records prepared to prevent or respond to emergency situations identifying or describing the name, location, pharmaceutical cache, contents, capacity, equipment, physical features, or capabilities of individual medical facilities, storage facilities, or laboratories.(2) The custodian may deny inspection of a part of a public record under paragraph (1) of this subsection only to the extent that the inspection would:(i) jeopardize the security of any building, structure, or facility;(ii) facilitate the planning of a terrorist attack; or (iii) endanger the life or physical safety of an individual.(3) (i) Subject to subparagraph (ii) of this paragraph, a custodian may not deny inspection of a public record under paragraph (1) or (2) of

this subsection that relates to a building, structure, or facility that has been subjected to a catastrophic event, including a fire, explosion, or natural disaster.(ii) This paragraph does not apply to the records of any building, structure, or facility owned or operated by the State or any of its political subdivisions.(4) (i) Subject to paragraphs (1) and (2) of this subsection and subparagraph (ii) of this paragraph, a custodian may not deny inspection of a public record that relates to an inspection of or issuance of a citation concerning a building, structure, or facility by an agency of the State or any political subdivision.(ii) This paragraph does not apply to the records of any building, structure, or facility owned or operated by the State or any of its political subdivisions.

(k) *Denial of inspection of public record.*—(1) A custodian may deny inspection of any part of a public record that contains:(i) stevedoring or terminal services or facility use rates or proposed rates generated, received, or negotiated by the Maryland Port Administration or any private operating company created by the Maryland Port Administration;(ii) a proposal generated, received, or negotiated by the Maryland Port Administration or any private operating company created by the Maryland Port Administration for use of stevedoring or terminal services or facilities to increase waterborne commerce through the ports of the State; or(iii) except as provided in paragraph (2) of this subsection, research or analysis related to maritime businesses or vessels compiled for the Maryland Port Administration or any private operating company created by the Maryland Port Administration to evaluate its competitive position with respect to other ports.(2) (i) A custodian may not deny inspection of any part of a public record under paragraph (1) (iii) of this subsection by the exclusive representative identified in Section 1 of the memorandum of understanding, or any identical section of a successor memorandum, between the State and the American Federation of State, County and Municipal Employees dated June 28, 2000 or the memorandum of understanding, or any identical section of a successor memorandum, between the State and the Maryland Professional Employees Council dated August 18, 2000 if the part of the public record:1. is related to State employees; and

2. would otherwise be available to the exclusive representative under Article 4, Section 12 of the memorandum of understanding or any identical section of a successor memorandum of understanding. (ii) Before the inspection of any part of a public record under subparagraph (i) of this paragraph, the exclusive representative shall enter into a nondisclosure agreement with the Maryland Port Administration to ensure the confidentiality of the information provided.

Missouri Revised State Statutes

Chapter 610: Governmental Bodies and Records

Section 610.021: Closed meetings and closed records authorized when, exceptions, sunset dates for certain exceptions.

610.021. Except to the extent disclosure is otherwise required by law, a public governmental body is authorized to close meetings, records and votes, to the extent they relate to the following:

(1) Legal actions, causes of action or litigation involving a public governmental body and any confidential or privileged communications between a public governmental body or its representatives and its attorneys. However, any minutes, vote or settlement agreement relating to legal actions, causes of action or litigation involving a public governmental body or any agent or entity representing its interests or acting on its behalf or with its authority, including any insurance company acting on behalf of a public government body as its insured, shall be made public upon final disposition of the matter voted upon or upon the signing by the parties of the settlement agreement, unless, prior to final disposition, the settlement agreement is ordered closed by a court after a written finding that the adverse impact to a plaintiff or plaintiffs to the action clearly outweighs the public policy considerations of section 610.011, however, the amount of any moneys paid by, or on behalf of, the public governmental body shall be disclosed; provided, however, in matters involving the exercise of the power of eminent domain, the vote shall be announced or become public immediately following the action on the motion to authorize institution of such a legal action. Legal work product shall be considered a closed record;

(2) Leasing, purchase or sale of real estate by a public governmental body where public knowledge of the transaction might adversely affect the legal consideration therefor. However, any minutes, vote or public record approving a contract relating to the leasing, purchase or sale of real estate by a public governmental body shall be made public upon execution of the lease, purchase or sale of the real estate;

(3) Hiring, firing, disciplining or promoting of particular employees by a public governmental body when personal information about the employee is discussed or recorded. However, any vote on a final decision, when taken by a public governmental body, to hire, fire, promote or discipline an employee of a public governmental body shall be made available with a record of how each member voted to the public within seventy-two hours of the close of the meeting where such action occurs; provided, however, that any employee so affected shall be entitled to prompt notice of such decision during the seventy-two-hour period before such decision is made available to the public. As used in this subdivision, the term “personal information” means information relating to the performance or merit of individual employees;

(4) The state militia or national guard or any part thereof;

(5) Nonjudicial mental or physical health proceedings involving identifiable persons, including medical, psychiatric, psychological, or alcoholism or drug dependency diagnosis or treatment;

(6) Scholastic probation, expulsion, or graduation of identifiable individuals, including records of individual test or examination scores; however, personally identifiable student records maintained by public educational institutions shall be open for inspection by the parents, guardian or other custodian of students under the age of eighteen years and by the parents, guardian or other custodian and the student if the student is over the age of eighteen years;

(7) Testing and examination materials, before the test or examination is given or, if it is to be given again, before so given again;

(8) Welfare cases of identifiable individuals;

(9) Preparation, including any discussions or work product, on behalf of a public governmental body or its representatives for negotiations with employee groups;

(10) Software codes for electronic data processing and documentation thereof;

(11) Specifications for competitive bidding, until either the specifications are officially approved by the public governmental body or the specifications are published for bid;

(12) Sealed bids and related documents, until the bids are opened; and sealed proposals and related documents or any documents related to a negotiated contract until a contract is executed, or all proposals are rejected;

(13) Individually identifiable personnel records, performance ratings or records pertaining to employees or applicants for employment, except that this exemption shall not apply to the names, positions, salaries and lengths of service of officers and employees of public agencies once they are employed as such, and the names of private sources donating or contributing money to the salary of a chancellor or president at all public colleges and universities in the state of Missouri and the amount of money contributed by the source;

(14) Records which are protected from disclosure by law;

(15) Meetings and public records relating to scientific and technological innovations in which the owner has a proprietary interest;

(16) Records relating to municipal hotlines established for the reporting of abuse and wrongdoing;

(17) Confidential or privileged communications between a public governmental body and its auditor, including all auditor work product; however, all final audit reports issued by the auditor are to be considered open records pursuant to this chapter;

*(18) Operational guidelines and policies developed, adopted, or maintained by any public agency responsible for law enforcement, public safety, first response, or public health for use in responding to or preventing any critical incident which is or appears to be terrorist in nature and which has the potential to endanger individual or public

*Subsections 18 and 19 of this section expire 12-31-08

safety or health. 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. When seeking to close information pursuant to this exception, the agency shall affirmatively state in writing that disclosure would impair its ability to protect the safety or health of persons, and shall in the same writing state that the public interest in nondisclosure outweighs the public interest in disclosure of the records. This exception shall sunset on December 31, 2008;

*(19) Existing or proposed security systems and structural plans of real property owned or leased by a public governmental body, and information that is voluntarily submitted by a nonpublic entity owning or operating an infrastructure to any public governmental body for use by that body to devise plans for protection of that infrastructure, the public disclosure of which would threaten public safety:

(a) Records related to the procurement of or expenditures relating to security systems purchased with public funds shall be open;

(b) When seeking to close information pursuant to this exception, the public governmental body shall affirmatively state in writing that disclosure would impair the public governmental body's ability to protect the security or safety of persons or real property, and shall in the same writing state that the public interest in nondisclosure outweighs the public interest in disclosure of the records;

(c) Records that are voluntarily submitted by a nonpublic entity shall be reviewed by the receiving agency within ninety days of submission to determine if retention of the document is necessary in furtherance of a state security interest. If retention is not necessary, the documents shall be returned to the nonpublic governmental body or destroyed;

(d) This exception shall sunset on December 31, 2008;

(20) Records that identify the configuration of components or the operation of a computer, computer system, computer network, or telecommunications network, and would allow unauthorized access to or unlawful disruption of a computer, computer system, computer network, or telecommunications network of a public governmental body. This exception shall not be used to limit or deny access to otherwise public records in a file, document, data file or database containing public records. Records related to the procurement of or expenditures relating to such computer, computer system, computer network, or telecommunications network, including the amount of moneys paid by, or on behalf of, a public governmental body for such computer, computer system, computer network, or telecommunications network shall be open; and

(21) Credit card numbers, personal identification numbers, digital certificates, physical and virtual keys, access codes or authorization codes that are used to protect the security of electronic transactions between a public governmental body and a person or entity doing business with a public governmental body. Nothing in this section shall be deemed to close the record of a person or entity using a credit card held in the name of a public governmental body or any record of a transaction made by a person using a credit card or other method of payment for which reimbursement is made by a public governmental body.

Texas Government Code

Chapter 418. Emergency Management

Sec. 418.177. CONFIDENTIALITY OF CERTAIN INFORMATION RELATING TO RISK OR VULNERABILITY ASSESSMENT. Information is confidential if the information:

(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.

Added by Acts 2003, 78th Leg., ch. 1312, Sec. 3, eff. June 21, 2003.

Code of Virginia

§ 2.2-3705.2. Exclusions to application of chapter; records relating to public safety.

The following records are excluded from the provisions of this chapter but may be disclosed by the custodian in his discretion, except where such disclosure is prohibited by law:

1. Confidential records, including victim identity, provided to or obtained by staff in a rape crisis center or a program for battered spouses.

2. Those portions of engineering and construction drawings and plans submitted for the sole purpose of complying with the Building Code in obtaining a building permit that would identify specific trade secrets or other information, the disclosure of which would be harmful to the competitive position of the owner or lessee. However, such information shall be exempt only until the building is completed. Information relating to the safety or environmental soundness of any building shall not be exempt from disclosure.

Those portions of engineering and construction drawings and plans that reveal critical structural components, security equipment and systems, ventilation systems, fire protection equipment, mandatory building emergency equipment or systems, elevators, electrical systems, telecommunications equipment and systems, and other utility equipment and systems submitted for the purpose of complying with the Uniform Statewide Building Code (§ 36-97 et seq.) or the Statewide Fire Prevention Code (§ 27-94 et seq.), the disclosure of which would jeopardize the safety or security of any public or private commercial office, multifamily residential or retail building or its occupants in the event of terrorism or other threat to public safety, to the extent that the owner or lessee of such property, equipment or system in writing (i) invokes the protections of this paragraph; (ii) identifies the drawings, plans, or other materials to be protected; and (iii) states the reasons why protection is necessary.

Nothing in this subdivision shall prevent the disclosure of information relating to any building in connection with an inquiry into the performance of that building after it has been subjected to fire, explosion, natural disaster or other catastrophic event.

3. Documentation or other information that describes the design, function, operation or access control features of any security system, whether manual or automated, which is used to control access to or use of any automated data processing or telecommunications system.

4. Plans and information to prevent or respond to terrorist activity, the disclosure of which would jeopardize the safety of any person, including (i) critical infrastructure sector or structural components; (ii) vulnerability assessments, operational, procedural, transportation, and tactical planning or training manuals, and staff meeting minutes or other records; and (iii) engineering or architectural records, or records containing information derived from such records, to the extent such records 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, structure or information storage facility, or telecommunications or utility equipment or systems. The same categories of records of any governmental or nongovernmental person or entity submitted to a public body for the purpose of antiterrorism response planning may be withheld from disclosure if such person or entity in writing (a) invokes the protections of this subdivision, (b) identifies with specificity the records or portions thereof for which protection is sought, and (c) states with reasonable particularity why the protection of such records from public disclosure is necessary to meet the objective of antiterrorism planning or protection. Such statement shall be a public record and shall be disclosed upon request. Nothing in this subdivision shall be construed to prohibit the disclosure of records relating to the structural or environmental soundness of any building, nor shall it prevent the disclosure of information relating to any building in connection with an inquiry into the performance of that building after it has been subjected to fire, explosion, natural disaster or other catastrophic event.

5. Information that would disclose the security aspects of a system safety program plan adopted pursuant to 49 C.F.R. Part 659 by the Commonwealth's designated Rail Fixed Guideway Systems Safety Oversight agency; and information in the possession of such agency, the release of which would jeopardize the success of an ongoing investigation of a rail accident or other incident threatening railway safety.

6. Engineering and architectural drawings, operational, procedural, tactical planning or training manuals, or staff meeting minutes or other records, the disclosure of which would reveal surveillance techniques, personnel deployments, alarm or security systems or technologies, 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.

7. Security plans and specific assessment components of school safety audits, as provided in § 22.1-279.8.

Nothing in this subdivision shall be construed to prohibit the disclosure of records relating to the effectiveness of security plans after (i) any school building or property has been subjected to fire, explosion, natural disaster or other catastrophic event, or (ii) any person on school property has suffered or been threatened with any personal injury.

8. (Expires July 1, 2006) Records of the Virginia Commission on Military Bases created by the Governor pursuant to Executive Order No. 49 (2003), to the extent that such records contain information relating to vulnerabilities of military bases located in Virginia and strategies under consideration or developed by the Commission to limit the effect of or to prevent the realignment or closure of federal military bases located in Virginia.

9. Records of the Commitment Review Committee concerning the mental health assessment of an individual subject to commitment as a sexually violent predator under Article 1.1 (§ 37.1-70.1 et seq.) of Chapter 2 of Title 37.1; except that in no case shall records identifying the victims of a sexually violent predator be disclosed.

10. Subscriber data, which for the purposes of this subdivision, means the name, address, telephone number, and any other information identifying a subscriber of a telecommunications carrier, provided directly or indirectly by a telecommunications carrier to a public body that operates a 911 or E-911 emergency dispatch system or an emergency notification or reverse 911 system, if the data is in a form not made available by the telecommunications carrier to the public generally. Nothing in this subdivision shall prevent the release of subscriber data generated in connection with specific calls to a 911 emergency system, where the requester is seeking to obtain public records about the use of the system in response to a specific crime, emergency or other event as to which a citizen has initiated a 911 call.

Revised Code of Washington

RCW 42.17.310 Certain personal and other records exempt

(1) The following are exempt from public inspection and copying:

(a) Personal information in any files maintained for students in public schools, patients or clients of public institutions or public health agencies, or welfare recipients.

(b) Personal information in files maintained for employees, appointees, or elected officials of any public agency to the extent that disclosure would violate their right to privacy.

(c) Information required of any taxpayer in connection with the assessment or collection of any tax if the disclosure of the information to other persons would (i) be prohibited to such persons by RCW 84.08.210, 82.32.330, 84.40.020, or 84.40.340 or (ii) violate the taxpayer's right to privacy or result in unfair competitive disadvantage to the taxpayer.

(d) Specific intelligence information and specific investigative records compiled by investigative, law enforcement, and penology agencies, and state agencies vested with the responsibility to discipline members of any profession, the nondisclosure of which is essential to effective law enforcement or for the protection of any person's right to privacy.

(e) Information revealing the identity of persons who are witnesses to or victims of crime or who file complaints with investigative, law enforcement, or penology agencies, other than the public disclosure commission, if disclosure would endanger any person's life, physical safety, or property. If at the time a complaint is filed the complainant, victim or witness indicates a desire for disclosure or nondisclosure, such desire shall govern. However, all complaints filed with the public disclosure commission about any elected official or candidate for public office must be made in writing and signed by the complainant under oath.

(f) Test questions, scoring keys, and other examination data used to administer a license, employment, or academic examination.

(g) Except as provided by chapter 8.26 RCW, the contents of real estate appraisals, made for or by any agency relative to the acquisition or sale of property, until the project or prospective sale is abandoned or until such time as all of the property has been acquired or the property to which the sale appraisal relates is sold, but in no event shall disclosure be denied for more than three years after the appraisal.

(h) Valuable formulae, designs, drawings, computer source code or object code, and research data obtained by any agency within five years of the request for disclosure when disclosure would produce private gain and public loss.

(i) Preliminary drafts, notes, recommendations, and intra-agency memorandums in which opinions are expressed or policies formulated or recommended except that a

specific record shall not be exempt when publicly cited by an agency in connection with any agency action.

(j) Records which are relevant to a controversy to which an agency is a party but which records would not be available to another party under the rules of pretrial discovery for causes pending in the superior courts.

(k) Records, maps, or other information identifying the location of archaeological sites in order to avoid the looting or depredation of such sites.

(l) Any library record, the primary purpose of which is to maintain control of library materials, or to gain access to information, which discloses or could be used to disclose the identity of a library user.

(m) Financial information supplied by or on behalf of a person, firm, or corporation for the purpose of qualifying to submit a bid or proposal for (i) a ferry system construction or repair contract as required by RCW 47.60.680 through 47.60.750 or (ii) highway construction or improvement as required by RCW 47.28.070.

(n) Railroad company contracts filed prior to July 28, 1991, with the utilities and transportation commission under *RCW 81.34.070, except that the summaries of the contracts are open to public inspection and copying as otherwise provided by this chapter.

(o) Financial and commercial information and records supplied by private persons pertaining to export services provided pursuant to chapter 43.163 RCW and chapter 53.31 RCW, and by persons pertaining to export projects pursuant to RCW 43.23.035.

(p) Financial disclosures filed by private vocational schools under chapters 28B.85 and 28C.10 RCW.

(q) Records filed with the utilities and transportation commission or attorney general under RCW 80.04.095 that a court has determined are confidential under RCW 80.04.095.

(r) Financial and commercial information and records supplied by businesses or individuals during application for loans or program services provided by chapters 43.163, 43.160, 43.330, and 43.168 RCW, or during application for economic development loans or program services provided by any local agency.

(s) Membership lists or lists of members or owners of interests of units in timeshare projects, subdivisions, camping resorts, condominiums, land developments, or common-interest communities affiliated with such projects, regulated by the department of licensing, in the files or possession of the department.

(t) All applications for public employment, including the names of applicants, resumes, and other related materials submitted with respect to an applicant.

(u) The residential addresses or residential telephone numbers of employees or volunteers of a public agency which are held by any public agency in personnel

records, public employment related records, or volunteer rosters, or are included in any mailing list of employees or volunteers of any public agency.

(v) The residential addresses and residential telephone numbers of the customers of a public utility contained in the records or lists held by the public utility of which they are customers, except that this information may be released to the division of child support or the agency or firm providing child support enforcement for another state under Title IV-D of the federal social security act, for the establishment, enforcement, or modification of a support order.

(w)(i) The federal social security number of individuals governed under chapter 18.130 RCW maintained in the files of the department of health, except this exemption does not apply to requests made directly to the department from federal, state, and local agencies of government, and national and state licensing, credentialing, investigatory, disciplinary, and examination organizations; (ii) the current residential address and current residential telephone number of a health care provider governed under chapter 18.130 RCW maintained in the files of the department, if the provider requests that this information be withheld from public inspection and copying, and provides to the department an accurate alternate or business address and business telephone number. On or after January 1, 1995, the current residential address and residential telephone number of a health care provider governed under RCW 18.130.040 maintained in the files of the department shall automatically be withheld from public inspection and copying unless the provider specifically requests the information be released, and except as provided for under RCW 42.17.260(9).

(x) Information obtained by the board of pharmacy as provided in RCW 69.45.090.

(y) Information obtained by the board of pharmacy or the department of health and its representatives as provided in RCW 69.41.044, 69.41.280, and 18.64.420.

(z) Financial information, business plans, examination reports, and any information produced or obtained in evaluating or examining a business and industrial development corporation organized or seeking certification under chapter 31.24 RCW.

(aa) Financial and commercial information supplied to the state investment board by any person when the information relates to the investment of public trust or retirement funds and when disclosure would result in loss to such funds or in private loss to the providers of this information.

(bb) Financial and valuable trade information under RCW 51.36.120.

(cc) Client records maintained by an agency that is a domestic violence program as defined in RCW 70.123.020 or 70.123.075 or a rape crisis center as defined in RCW 70.125.030.

(dd) Information that identifies a person who, while an agency employee: (i) Seeks advice, under an informal process established by the employing agency, in order to ascertain his or her rights in connection with a possible unfair practice under chapter 49.60 RCW against the person; and (ii) requests his or her identity or any identifying information not be disclosed.

(ee) Investigative records compiled by an employing agency conducting a current investigation of a possible unfair practice under chapter 49.60 RCW or of a possible violation of other federal, state, or local laws prohibiting discrimination in employment.

(ff) Business related information protected from public inspection and copying under RCW 15.86.110.

(gg) Financial, commercial, operations, and technical and research information and data submitted to or obtained by the clean Washington center in applications for, or delivery of, program services under chapter 70.95H RCW.

(hh) Information and documents created specifically for, and collected and maintained by a quality improvement committee pursuant to RCW 43.70.510 or 70.41.200, or by a peer review committee under RCW 4.24.250, regardless of which agency is in possession of the information and documents.

(ii) Personal information in files maintained in a data base created under **RCW 43.07.360.

(jj) Financial and commercial information requested by the public stadium authority from any person or organization that leases or uses the stadium and exhibition center as defined in RCW 36.102.010.

(kk) Names of individuals residing in emergency or transitional housing that are furnished to the department of revenue or a county assessor in order to substantiate a claim for property tax exemption under RCW 84.36.043.

(ll) The names, residential addresses, residential telephone numbers, and other individually identifiable records held by an agency in relation to a vanpool, carpool, or other ride-sharing program or service. However, these records may be disclosed to other persons who apply for ride-matching services and who need that information in order to identify potential riders or drivers with whom to share rides.

(mm) The personally identifying information of current or former participants or applicants in a paratransit or other transit service operated for the benefit of persons with disabilities or elderly persons.

(nn) The personally identifying information of persons who acquire and use transit passes and other fare payment media including, but not limited to, stored value smart cards and magnetic strip cards, except that an agency may disclose this information to a person, employer, educational institution, or other entity that is responsible, in whole or in part, for payment of the cost of acquiring or using a transit pass or other fare payment media, or to the news media when reporting on public transportation or public safety. This information may also be disclosed at the agency's discretion to governmental agencies or groups concerned with public transportation or public safety.

(oo) Proprietary financial and commercial information that the submitting entity, with review by the department of health, specifically identifies at the time it is submitted and that is provided to or obtained by the department of health in

connection with an application for, or the supervision of, an antitrust exemption sought by the submitting entity under RCW 43.72.310. If a request for such information is received, the submitting entity must be notified of the request. Within ten business days of receipt of the notice, the submitting entity shall provide a written statement of the continuing need for confidentiality, which shall be provided to the requester. Upon receipt of such notice, the department of health shall continue to treat information designated under this section as exempt from disclosure. If the requester initiates an action to compel disclosure under this chapter, the submitting entity must be joined as a party to demonstrate the continuing need for confidentiality.

(pp) Records maintained by the board of industrial insurance appeals that are related to appeals of crime victims' compensation claims filed with the board under RCW 7.68.110.

(qq) Financial and commercial information supplied by or on behalf of a person, firm, corporation, or entity under chapter 28B.95 RCW relating to the purchase or sale of tuition units and contracts for the purchase of multiple tuition units.

(rr) Any records of investigative reports prepared by any state, county, municipal, or other law enforcement agency pertaining to sex offenses contained in chapter 9A.44 RCW or sexually violent offenses as defined in RCW 71.09.020, which have been transferred to the Washington association of sheriffs and police chiefs for permanent electronic retention and retrieval pursuant to RCW 40.14.070(2)(b).

(ss) Credit card numbers, debit card numbers, electronic check numbers, card expiration dates, or bank or other financial account numbers, except when disclosure is expressly required by or governed by other law.

(tt) Financial information, including but not limited to account numbers and values, and other identification numbers supplied by or on behalf of a person, firm, corporation, limited liability company, partnership, or other entity related to an application for a liquor license, gambling license, or lottery retail license.

(uu) Records maintained by the employment security department and subject to chapter 50.13 RCW if provided to another individual or organization for operational, research, or evaluation purposes.

(vv) Individually identifiable information received by the work force training and education coordinating board for research or evaluation purposes.

(ww) 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.

(xx) Commercial fishing catch data from logbooks required to be provided to the department of fish and wildlife under RCW 77.12.047, when the data identifies specific catch location, timing, or methodology and the release of which would result in unfair competitive disadvantage to the commercial fisher providing the catch data. However, this information may be released to government agencies concerned with the management of fish and wildlife resources.

(yy) Sensitive wildlife data obtained by the department of fish and wildlife. However, sensitive wildlife data may be released to government agencies concerned with the management of fish and wildlife resources. Sensitive wildlife data includes:

(i) The nesting sites or specific locations of endangered species designated under RCW 77.12.020, or threatened or sensitive species classified by rule of the department of fish and wildlife;

(ii) Radio frequencies used in, or locational data generated by, telemetry studies; or

(iii) Other location data that could compromise the viability of a specific fish or wildlife population, and where at least one of the following criteria are met:

(A) The species has a known commercial or black market value;

(B) There is a history of malicious take of that species; or

(C) There is a known demand to visit, take, or disturb, and the species behavior or ecology renders it especially vulnerable or the species has an extremely limited distribution and concentration.

(zz) The personally identifying information of persons who acquire recreational licenses under RCW 77.32.010 or commercial licenses under chapter 77.65 or 77.70 RCW, except name, address of contact used by the department, and type of license, endorsement, or tag. However, the department of fish and wildlife may disclose personally identifying information to:

(i) Government agencies concerned with the management of fish and wildlife resources;

(ii) The department of social and health services, child support division, and to the department of licensing in order to implement RCW 77.32.014 and 46.20.291; and

(iii) Law enforcement agencies for the purpose of firearm possession enforcement under RCW 9.41.040.

(aaa)(i) Discharge papers of a veteran of the armed forces of the United States filed at the office of the county auditor before July 1, 2002, that have not been commingled with other recorded documents. These records will be available only to the veteran,

the veteran's next of kin, a deceased veteran's properly appointed personal representative or executor, a person holding that veteran's general power of attorney, or to anyone else designated in writing by that veteran to receive the records.

(ii) Discharge papers of a veteran of the armed forces of the United States filed at the office of the county auditor before July 1, 2002, that have been commingled with other records, if the veteran has recorded a "request for exemption from public disclosure of discharge papers" with the county auditor. If such a request has been recorded, these records may be released only to the veteran filing the papers, the veteran's next of kin, a deceased veteran's properly appointed personal representative or executor, a person holding the veteran's general power of attorney, or anyone else designated in writing by the veteran to receive the records.

(iii) Discharge papers of a veteran filed at the office of the county auditor after June 30, 2002, are not public records, but will be available only to the veteran, the veteran's next of kin, a deceased veteran's properly appointed personal representative or executor, a person holding the veteran's general power of attorney, or anyone else designated in writing by the veteran to receive the records.

(iv) For the purposes of this subsection (1)(aaa), next of kin of deceased veterans have the same rights to full access to the record. Next of kin are the veteran's widow or widower who has not remarried, son, daughter, father, mother, brother, and sister.

(bbb) 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.

(ccc) Information compiled by school districts or schools in the development of their comprehensive safe school plans pursuant to RCW 28A.320.125, to the extent that they identify specific vulnerabilities of school districts and each individual school.

(ddd) 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.

(eee) Information obtained and exempted or withheld from public inspection by the health care authority under RCW 41.05.026, whether retained by the authority, transferred to another state purchased health care program by the authority, or transferred by the authority to a technical review committee created to facilitate the development, acquisition, or implementation of state purchased health care under chapter 41.05 RCW.

(fff) Proprietary data, trade secrets, or other information that relates to: (i) A vendor's unique methods of conducting business; (ii) data unique to the product or services of the vendor; or (iii) determining prices or rates to be charged for services, submitted by any vendor to the department of social and health services for purposes of the

development, acquisition, or implementation of state purchased health care as defined in RCW 41.05.011.

(ggg) Proprietary information deemed confidential for the purposes of section 923, chapter 26, Laws of 2003 1st sp. sess.

(2) Except for information described in subsection (1)(c)(i) of this section and confidential income data exempted from public inspection pursuant to RCW 84.40.020, the exemptions of this section are inapplicable to the extent that information, the disclosure of which would violate personal privacy or vital governmental interests, can be deleted from the specific records sought. No exemption may be construed to permit the nondisclosure of statistical information not descriptive of any readily identifiable person or persons.

(3) Inspection or copying of any specific records exempt under the provisions of this section may be permitted if the superior court in the county in which the record is maintained finds, after a hearing with notice thereof to every person in interest and the agency, that the exemption of such records is clearly unnecessary to protect any individual's right of privacy or any vital governmental function.

(4) Agency responses refusing, in whole or in part, inspection of any public record shall include a statement of the specific exemption authorizing the withholding of the record (or part) and a brief explanation of how the exemption applies to the record withheld.

Abbreviations used without definitions in TRB publications:

AASHO	American Association of State Highway Officials
AASHTO	American Association of State Highway and Transportation Officials
APTA	American Public Transportation Association
ASCE	American Society of Civil Engineers
ASME	American Society of Mechanical Engineers
ASTM	American Society for Testing and Materials
ATA	American Trucking Associations
CTAA	Community Transportation Association of America
CTBSSP	Commercial Truck and Bus Safety Synthesis Program
DHS	Department of Homeland Security
FAA	Federal Aviation Administration
FHWA	Federal Highway Administration
FMCSA	Federal Motor Carrier Safety Administration
FRA	Federal Railroad Administration
FTA	Federal Transit Administration
IEEE	Institute of Electrical and Electronics Engineers
ITE	Institute of Transportation Engineers
NCHRP	National Cooperative Highway Research Program
NCTRP	National Cooperative Transit Research and Development Program
NHTSA	National Highway Traffic Safety Administration
NTSB	National Transportation Safety Board
SAE	Society of Automotive Engineers
TCRP	Transit Cooperative Research Program
TRB	Transportation Research Board
TSA	Transportation Security Administration
U.S.DOT	United States Department of Transportation