1989

Session Law 89-014

Florida Senate & House of Representatives

Florida Information Associates
Florida Legislature
Staff Analyses
1989 Sessions

89-14

S 98 GENERAL BILL/1ST ENG by Governmental Operations (Identical 1ST ENG/H 1695)

Security of Data: (OPEN GOVERNMENT SUNSET REVIEW) continues exemption of risk-analysis information & internal audits & evaluations from public records requirements of public records law; continues, with modifications, such exemption for written internal policies & procedures; provides for future legislative review. Amends 282.318. Effective Date: 10/01/89.

BILL HISTORY

01/12/89	SENATE	Prefiled
02/13/89	SENATE	Referred to Governmental Operations
03/07/89	SENATE	On Committee agenda—Governmental Operations, 03/07/89, 1:15 pm, Room-H—Not considered
04/04/89	SENATE	Introduced, referred to Governmental Operations -SJ 15; On Committee agenda—Governmental Operations, 04/06/89, 3:15 pm, Room-H-(428)
04/06/89	SENATE	Comm. Report: Favorable by Governmental Operations, placed on Calendar -SJ 117
04/18/89	SENATE	Placed on Special Order Calendar -SJ 173
04/25/89	SENATE	Placed on Special Order Calendar -SJ 198; Passed; YEAS 37 NAYS 0 -SJ 206
04/27/89	SENATE	Immediately certified -SJ 229
04/27/89	HOUSE	In Messages
04/28/89	HOUSE	Received, placed on Calendar -HJ 297; Substituted for HB 1695 -HJ 302; Read second time; Amendment adopted; Read third time; Passed as amended; YEAS 109 NAYS 0 -HJ 303
05/02/89	SENATE	In Messages
05/09/89	SENATE	Concurred; Passed as amended; YEAS 35 NAYS 0 -SJ 279
05/09/89		Ordered engrossed, then enrolled -SJ 279
05/16/89		Signed by Officers and presented to Governor -SJ 378
05/22/89		Approved by Governor; Chapter No. 89-14 -SJ 414

NOTES: Above bill history from Division of Legislative Information's *FINAL LEGISLATIVE BILL INFORMATION, 1989 SESSIONS*. Staff Analyses for bills amended beyond final committee action may not be in accordance with the enacted law. Journal page numbers (HJ & SJ) refer to daily Journals and may not be the same as final bound Journals.

REVISED: _____ BILL NO. SB 98

DATE: April 6, 1989 Page 1

SENATE STAFF ANALYSIS AND ECONOMIC IMPACT STATEMENT

	ANALYST	STAFF DIRECTOR		REFERENCE	ACTION
1.	Kane	Stengle	1.	GO	Favorable
2.			2.		
3.			3.		
4.			4.		

SUBJECT:

Open Government;
Security of Data and
Information Technology Resources

BILL NO. AND SPONSOR:

SB 98 by
Governmental Operations

I. SUMMARY:

A. Present Situation:

The Open Government Sunset Review Act provides for the repeal of public meetings and public records exemptions over the 10-year period from 1986-1995, unless the Legislature acts to revive an exemption prior to its scheduled repeal date. Section 282.318, F.S., requires the departments of the executive branch to take specific measures to ensure the security of departmental data and information technology resources. The law provides that three elements of the statutorily-required security programs are confidential information and are exempt from the provisions of ch. 119, F.S., relating to public records. No exemption is provided from the Public Meetings Law, s. 286.011, F.S.

Chapter 119, F.S., the Public Records Law, requires government records to be open to public inspection and copying, except as otherwise specifically exempted by law. Therefore, the exemptions contained in s. 282.318(3)(a)2., 3., and 5., F.S., require affected state agencies to keep specified elements of their security programs for data and information technology resources confidential.

Section 119.14, F.S., provides for legislative review of public meetings and public records exemptions prior to their scheduled repeal. During the course of the review of these exemptions, a questionnaire was sent to the 28 executive branch departments named in s. 282.318, F.S., as having responsibilities for maintaining measures for security of data and information technology resources, in order to gather information relative to agency computer security programs. Twenty-five of the 28 agencies surveyed responded to the questionnaire. Out of the 25 responses, 18 were sufficiently detailed and responsive to the questions posed so as to lend themselves to analysis for the purposes of the review. Another questionnaire was sent to the Information Resource Commission to obtain the commission's analysis of the need for the exemptions.

Chapter 282, F.S., is designated as the "Information Resources Management Act." The law provides for effective management, planning, and use of information resources. Section 282.304, F.S., creates the Information Resources Commission (commission), comprised of the Governor and Cabinet, to centralize planning and policy for information resources for the executive branch of state government. Among other assigned functions, the commission is directed to develop policies and procedures relating to information resources management, provide information resources management training programs, and provide agencies with technical and managerial services upon request.

Section 282.318, F.S., is designated as the "Security of Data and Information Technology Resources Act." Section 282.303(10), F.S., defines "information technology resources" as "data processing hardware and software and services, supplies, personnel, facility resources, maintenance, and training." The term "data" is defined by draft guidelines of the commission as "a representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means."

Section 282.318, F.S., requires each executive branch department, as defined by ch. 20, F.S., to take specific measures to ensure the security of departmental data and information technology resources. The law is also made specifically applicable to the State Board of Administration, the Executive Office of the Governor, and the Game and Fresh Water Fish Commission. Section 282.318(3)(a)1.-8., F.S., specifies eight actions required at a minimum to establish a program for computer security. These requirements include conducting periodic risk analyses to identify security threats to data and information technology resources, developing and maintaining written internal security policies and procedures, and conducting periodic audits and evaluations of the security program. Subparagraphs 2., 3., and 5., of s. 282.318(3)(a), F.S., which establish these particular requirements, also provide that the required risk analyses, written policies and procedures, and audit results are confidential, and are exempt from the public access provisions of ch. 119, F.S. The law requires that all three elements be updated periodically. Each department must annually certify to the commission that its security program conforms to the commission's guidelines, or the department must identify and explain any deviations.

The commission is directed to provide centralized management and coordination of state policies relating to computer security, including the establishment and maintenance of minimum standards, rules, and regulations to be followed by the departments in implementing the statutory requirements for computer security. The commission is in the process of developing guidelines with the help of, and in coordination with, all affected departments. In August 1988, the commission completed the third draft of Information Resources Security Standards and Guidelines, which have been distributed to the departments for comment. After opportunities for comments and modifications, the commission will submit its security policies and standards for adoption as rules, in conformance with ch. 120, F.S., the Administrative Procedure Act.

Security of data and information technology resources is a concept that is often confused with the separate task of maintaining the security of data designated by law as confidential. According to commission staff, the "security of data" means maintaining data integrity, "a state that exists when computerized information is the same as its source and has not been exposed to accidental or malicious alteration or destruction." All data and information technology resources, including hardware and software, must be preserved from destruction or modification by access that is either inadvertent or unauthorized. For example, the Florida Statutes are public record. The data base containing the text of the statutes must be preserved from unauthorized changes, although the data itself is not confidential.

Maintaining the confidentiality of confidential data is another aspect of computer security. Many agencies maintain data which by law is confidential or is exempted from the public records law. Some examples of such information include tax records, information concerning regulatory or criminal investigations, and trade secrets. The security programs in place to protect the integrity of all computer-maintained data also assist in

reducing the likelihood that confidential data designated by law will be improperly disclosed to the public.

Without the exemptions, security measures protecting data and information technology resources would be rendered ineffective. If the security policies and procedures, security risk analyses, and results of security audits were open to public scrutiny, knowledgeable persons could gain access to departmental systems, and ultimately could alter data. As well, inadequate security procedures could result in the inadvertent alteration of data contained in the public records.

The written internal policies and procedures concerning security, according to commission staff, encompass not only specific security precautions that should not be disclosed to the public, but also contain very broad guiding principles which do not need to be confidential. For example, policies requiring back-up records of information, or very general procedures to be used to safeguard computer hardware and software from dangers such as fire or theft, need not be confidential. Rather, these broad principles are more useful if they are very generally disseminated to agency staff.

Of the 18 agencies which replied responsively to the exemption review questionnaire, 16 have performed the required risk analyses. Thirteen have developed written internal policies and procedures, and 12 have performed internal audits of departmental security programs. An additional two agencies are currently developing the risk analyses, policies and procedures, and internal audit procedures.

Some agencies submitted detailed information on how the exempted records are maintained. Of the 11 agencies which provided this data, 5 indicated that the risk analyses, security policies and procedures, and internal audit results are maintained in hard copy form, and are kept in a locked cabinet or other secure area. Some agencies maintain the exempted data as computer records. For several of these agencies, the risk analysis is conducted through a software program, and the results are stored in a computer system. Costs for maintaining the exempted records are negligible.

The staff of the Senate Governmental Operations Committee has completed its review of the exemptions provided in s. 282.318(3)(a)2., 3., and 5., F.S., and has made recommendations pertaining to the future repeal of the exemptions as provided by the Open Government Sunset Review Act.

B. Effect of Proposed Changes:

The exemptions from the Public Records Law contained in subparagraphs 2., and 5., of s. 282.318(3)(a), F.S., pertaining to computer security risk analyses, and the results of internal computer security audits, would be revived and reenacted without modification.

The exemption contained in subparagraph 3. of s. 282.(3)(a), F.S., pertaining to written internal computer security policies and procedures would be revived and reenacted with a modification that would narrow the scope of that exemption. Confidentiality of written internal security policies and procedures would be limited to only those written internal policies and procedures which, if disclosed, would facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources.

II. ECONOMIC IMPACT AND FISCAL NOTE:

A. Public:

None.

B. Government:

None.

III. COMMENTS:

All departments replying responsively to the review questionnaire that was sent to gather information regarding the exemptions in s. 282.318(3)(a)2., 3., and 5., F.S., recommended that the Legislature reenact the exemptions. Thus, security risk analyses, written internal security policies and procedures, and results of internal security audits would be confidential, and not open to view by the public. The staff of the commission stated that repeal of the exemptions "would compromise the very essence of departmental security." According to one responding agency, "publication of . . . security features to the data base . . . would be the same as telling a thief which door to your house is easiest to break into."

The commission and the Department of Education recommended modifying the scope of the exemption for written internal policies and procedures, provided for in subparagraph 3. of s. 282.318(3)(a), F.S. These agencies pointed out that the internal security policies and procedures contain broad guiding principles which should be available to all personnel, and that confidentiality of those particular policies and procedures which should be generally available hinders training and awareness programs.

IV. AMENDMENTS:

None.

89-14

****AS PASSED BY THE 1989 LEGISLATURE****

STORAGE NAME: h1695-f.go
DATE: June 14, 1989

HOUSE OF REPRESENTATIVES
COMMITTEE ON GOVERNMENTAL OPERATIONS
FINAL STAFF ANALYSIS & ECONOMIC IMPACT STATEMENT

BILL #: HB 1695 (PCB GO 89-17) (enacted as SB 98)

RELATING TO: Confidentiality of Information Resource Technology Procedures

SPONSOR(S): Committee on Governmental Operations and Representative Martin

EFFECTIVE DATE: October 1, 1989

DATE BECAME LAW: May 22, 1989

CHAPTER #: 89-14, Laws of Florida

COMPANION BILL(S): SB 98 (identical)

OTHER COMMITTEES OF REFERENCE: (1)

(2)

****

I. SHORT SUMMARY:

Section 282.318(3), Florida Statutes, establishes the processes agencies will use to protect computer systems, specifically data and information technology resources. Several reports are required that contain information about an agency's computer security procedures; these reports are exempt from the public records law. This bill re-enacts those exemptions, with clarifying language added to the second exemption to limit the exemption to those written internal policies and procedures that could, if disclosed, facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources. Finally, this bill removes the requirement that agencies certify annually that their security programs conform to the Information Resource Commission's guidelines.

A. INTRODUCTION:

Public policy of Florida has greatly favored public access to governmental records and meetings. In fact, the "Sunshine State" has been a national leader in the area of open government. The law embodying the public's right of access to records is codified at s. 119.01, Florida Statutes:

> It is the policy of this state that all state, county, and municipal records shall at all times be open for a personal inspection by any person.

This provision is mandatory and any public official with custody of a nonexempt public record is required to disclose it to any

member of the public. Records are exempt from public disclosure pursuant to chapter 119, Florida Statutes, only if it is provided by law that the public records are confidential or are expressly exempted from disclosure by general or special law. Exemptions are found in s. 119.07(3), Florida Statutes, and in various special acts. The provision requiring meetings to be public does not identify specific exemptions within that section, but various exemptions are included throughout the statutes.

In 1984, the Legislature enacted the Open Government Sunset Review Act to prevent the erosion of Florida's open government policy caused by unjustified exemptions to the Act. As amended by chapter 85-301, Laws of Florida, the Act provides specific criteria for the evaluation of exemptions subject to repeal. The law provides for a two-pronged test. First, it requires consideration of four factors:

- What specific records or meetings are affected by the exemption?

- Whom does the exemption uniquely affect, as opposed to the general public?

- What is the identifiable public purpose or goal of the exemption?

- Can information contained in the records or discussed in the meeting be readily obtained by alternative means? If so, how?

Second, the law requires that the exemption will be maintained only if it serves an identifiable purpose. An identifiable public purpose is served when the exemption meets one of the following purposes and such purpose is considered significant enough to override the strong public policy of open government. To qualify as meeting a public purpose, an exemption must:

- allow the state or its political subdivisions to effectively and efficiently administer a governmental program, which administration would be significantly impaired without the exemption; or

- protect information of a sensitive personal nature concerning individuals if its release would be defamatory to such individuals or cause unwarranted damage to the good name or reputation of such individuals, or its release would jeopardize the safety of such individuals; or

- protect information of a confidential nature concerning entities which include formulas, patterns, devices, combination of devices, or compilation of information which is used to protect or further a business advantage over those who do not know or use it if its disclosure would injure the affected entity in the marketplace.

The review included in this report examines the following exemption(s):

s. 282.318(3)(a) 2., 3., and 5., Florida Statutes

B. PRESENT SITUATION:

Section 282.318(3), Florida Statutes, establishes the processes agencies use to protect computer systems, specifically data and information technology resources. "Information technology resources" include data processing hardware, software and services, supplies, personnel, facility resources, maintenance, training, or other related resources. In order to assure an adequate level of security for data and information technology resources, s. 282.318(3)(a), Florida Statutes, requires each department head to perform the following tasks:

2. Conduct, and periodically update, a comprehensive risk analysis to determine the security threats to the data and information technology resources.

3. Develop, and periodically update, written internal policies and procedures to assure the security of the data and information technology resources.

5. Ensure that periodic internal audits and evaluations of the security program for data and information technology resources are conducted.

The reports that result from these tasks are exempt from the public records law, although each agency head must make the information available to the Auditor General for performing his postauditing duties.

If these exemptions were repealed, the state could not effectively and efficiently administer government programs because agencies would not be able to maintain the integrity of their computer systems and protect data contained in those systems. The computer systems and the information stored in them could be destroyed, altered, or otherwise made suspect or useless. For example, if the results of a risk analysis were made public, an individual reading the analysis would know how to alter or destroy data, software, or hardware.

Staff sent questionnaires to 28 agencies, and 18 responded. Four of these 18 agencies accounted for approximately 60% of the total information resources management expenditures during fiscal year 1987-88. All agencies responding to the questionnaire wanted to continue the exemptions. The Department of Education suggested modifying the internal policies and procedures exemption to include only those policies and procedures that could, if disclosed, facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources.

This bill re-enacts each of these exemptions, with clarifying language added to s. 282.318(3)(a)3. This language would limit the exemption to those written internal policies and procedures that could, if disclosed, facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources.

Finally, s. 282.318(8), Florida Statutes, requires each department head to certify annually to the Information Resource Commission (IRC) that the agency's security program for data and information technology resources conforms with the standards, policies, and guidelines developed by the IRC. An IRC representative told committee staff agencies should not be required to conform with guidelines and that the word "guidelines" should be removed from the statutes.

C. EFFECT OF PROPOSED CHANGES:

This bill would revive and readopt the public records exemption provided by s. 282.318(3)(a)2., 3., and 5., Florida Statutes, effective October 1, 1989, and would require Sunset Review of the exemption in ten years, as provided by s. 119.14, Florida Statutes.

Section 282.318(3)(a)3., Florida Statutes, would be amended to limit the exemptions to only those written internal policies and procedures that could, if disclosed, facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources. Additionally, this bill removes the requirement that agency heads certify annually to the IRC that their agencies conform with IRC guidelines.

D. SECTION-BY-SECTION ANALYSIS AS ENACTED IN SB 98:

Section 1 -- Amends 282.318(3)(a), Florida Statutes, to retain the public records exemptions for reports that contain information about an agency's computer security procedures. Limits the exemption to only those written internal policies and procedures that could, if disclosed, facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources. Removes the requirement that agency heads certify annually to the IRC that their agencies conform with IRC guidelines.

Section 2 -- Provides an effective date of October 1, 1989.

II. FISCAL ANALYSIS & ECONOMIC IMPACT STATEMENT:

A. FISCAL IMPACT ON STATE AGENCIES/STATE FUNDS:

1. Non-recurring or First Year Start-Up Effects:

Not applicable.

2. Recurring or Annualized Continuation Effects:

Not applicable.

3. Long Run Effects Other Than Normal Growth:

Not applicable.

4. Appropriations Consequences:

Not applicable.

B. FISCAL IMPACT ON LOCAL GOVERNMENTS AS A WHOLE:

1. Non-recurring or First Year Start-Up Effects:

Not applicable.

2. Recurring or Annualized Continuation Effects:

Not applicable.

3. Long Run Effects Other Than Normal Growth:

Not applicable.

C. DIRECT ECONOMIC IMPACT ON PRIVATE SECTOR:

1. Direct Private Sector Costs:

Not applicable.

2. Direct Private Sector Benefits:

Not applicable.

3. Effects on Competition, Private Enterprise, and Employment Markets:

Not applicable.

D. FISCAL COMMENTS:

Not applicable.

III. LONG RANGE CONSEQUENCES:

The issues in this bill are not addressed in the State Comprehensive Plan.

IV. COMMENTS:

This legislation is consistent with the Governmental Operations Committee mission statement, specifically: "Review exemptions to public record and public meeting laws pursuant to the Open Government Sunset Review Act to determine whether the continued existence of each exemption is compelled by justifications strong enough to override Florida's strong public policy of open government."

The House's Issues Conference Policy Statements do not address open government sunset reviews.

V. SIGNATURES:

SUBSTANTIVE COMMITTEE:
Prepared by: Lyn Davis
Lyn Davis

Staff Director:
Barry Kling

SECOND COMMITTEE OF REFERENCE:
Prepared by:

Staff Director:

APPROPRIATIONS:
Prepared by:

Staff Director: