



# House of Representatives

General Assembly

**File No. 325**

February Session, 2008

Substitute House Bill No. 5816

*House of Representatives, March 31, 2008*

The Committee on Energy and Technology reported through REP. FONTANA, S. of the 87th Dist., Chairperson of the Committee on the part of the House, that the substitute bill ought to pass.

## ***AN ACT CONCERNING INTERNET SECURITY.***

Be it enacted by the Senate and House of Representatives in General Assembly convened:

1 Section 1. (NEW) (*Effective from passage*) As used in sections 1 to 3,  
2 inclusive, of this act:

3 (1) "Availability" means the timely and reliable access to and use of  
4 information created, generated, collected or maintained by a state  
5 agency;

6 (2) "Communications and information resources" means (A)  
7 procedures, equipment and software designed, built, operated and  
8 maintained to collect, record, process, store, retrieve, display and  
9 transmit information; and (B) associated personnel, including  
10 consultants and contractors;

11 (3) "Confidentiality" means the preservation of authorized  
12 restrictions on information access and disclosure, including the means

13 for protecting personal privacy and proprietary information;

14 (4) "Searchable web site" means a web site that allows the public to  
15 search or aggregate information;

16 (5) "Information security" means the protection of communication  
17 and information resources from unauthorized access, use, disclosure,  
18 disruption, modification or destruction to (A) prevent improper  
19 information modification or destruction; (B) preserve authorized  
20 restrictions on information access and disclosure; (C) ensure timely  
21 and reliable access to and use of information; and (D) maintain the  
22 confidentiality, integrity and availability of information;

23 (6) "Information security plan" means the plan developed by a state  
24 agency pursuant to sections 1 to 3, inclusive, of this act;

25 (7) "Institution of higher education" means a state-supported  
26 institution of higher education;

27 (8) "Integrity" means the prevention of improper information  
28 modification or destruction and ensuring information nonrepudiation  
29 and authenticity;

30 (9) "Expenditure of state funds" means the expenditure of all  
31 appropriated or nonappropriated funds by a state entity from the  
32 Treasury in forms including, but not limited to, grants, contracts,  
33 subcontracts, tax refunds, rebates or credits, excluding those which  
34 result from the overpayment of income tax, or expenditures pursuant  
35 to any compact between the Governor and a federally recognized  
36 Indian tribe or nation in this state. "Expenditure of state funds" shall  
37 not mean the transfer of funds between two state agencies or payments  
38 of state or federal assistance to an individual; and

39 (10) "Security incident" means an accidental or deliberative event  
40 that results in or constitutes an imminent threat of the unauthorized  
41 access, loss, disclosure, modification, disruption or destruction of  
42 communication and information resources.

43       Sec. 2. (NEW) (*Effective from passage*) The Governor shall appoint a  
44 chief information security officer with experience in security and risk  
45 management for communications and information resources. Said  
46 chief information security officer's duties shall include, but not be  
47 limited to, (1) developing and updating information security  
48 procedures, standards and guidelines for all state agencies; (2)  
49 ensuring the incorporation of and compliance with information  
50 security policies, standards and guidelines in the information security  
51 plans developed by state agencies pursuant to sections 1 to 3, inclusive,  
52 of this act; (3) directing information security audits and assessments in  
53 state agencies to ensure program compliance; (4) establishing and  
54 directing a risk management process to identify information security  
55 risks in state agencies and deploy risk mitigation strategies, processes  
56 and procedures; (5) reviewing and approving state agency information  
57 security plans annually; and (6) conducting information security  
58 awareness training programs.

59       Sec. 3. (NEW) (*Effective from passage*) (a) On or before the start of  
60 each fiscal year, each state agency shall develop an information  
61 security plan using the information security policies, standards and  
62 guidelines developed by the chief information security officer  
63 appointed pursuant to section 2 of this act. Said plans shall provide  
64 information security for the communication and information resources  
65 that support the operations and assets of each state agency.

66       (b) Information security plans developed pursuant to subsection (a)  
67 of this section shall include, but not be limited to (1) periodic  
68 assessments of the risk and magnitude of the harm that could result  
69 from a security incident; (2) a process for providing adequate  
70 information security for the communication and information resources  
71 of the state agency; (3) periodic security awareness training to inform  
72 the agency's employees and users of the agency's communication and  
73 information resources about information security risks and the  
74 responsibility of employees and users to comply with agency policies,  
75 standards and procedures designed to reduce those risks; (4) periodic  
76 vulnerability assessment testing and evaluation of the effectiveness of

77 information security for the state agency, which shall be performed not  
78 less than annually; (5) a process for detecting, reporting and  
79 responding to security incidents consistent with the information  
80 security standards, policies and guidelines issued by the chief  
81 information security officer; and (6) plans and procedures to ensure  
82 the continuity of operations for information resources that support the  
83 operations and assets of the state agency during a security incident.

84 (c) On or before the beginning of each new fiscal year, each state  
85 agency shall submit the information security plan developed pursuant  
86 to subsection (a) of this section to the chief information security officer  
87 for approval.

88 (d) If a state agency fails to submit an information security plan to  
89 the chief information security officer on or before the beginning of the  
90 new fiscal year or if the chief information security officer disapproves  
91 said plan, the officer shall notify the Governor and the agency head of  
92 the agency in question. If no plan has been approved by October first  
93 of any year, the officer may suspend the operation of said agency's  
94 communication and information resources until such plan has been  
95 submitted to and approved by the officer.

96 (e) Information security plans developed pursuant to this section  
97 may provide for a phase-in period not to exceed three years. Any plan  
98 providing for such a phase-in period shall include an implementation  
99 schedule for such period.

100 (f) On or before the beginning of each new fiscal year, the head of  
101 each state agency shall report to the chief information security officer  
102 on the development, implementation and, if applicable, compliance  
103 with the phase-in schedule of the state agency's security plan. On or  
104 before January 1, 2010, and annually thereafter, the chief information  
105 security officer shall report, in accordance with section 11-4a of the  
106 general statutes, to the Governor and the joint standing committee of  
107 the General Assembly having cognizance of matters relating to  
108 technology concerning the implementation of the provisions of plans  
109 developed pursuant to this section.

110       Sec. 4. (NEW) (*Effective from passage*) (a) No later than January 1,  
111 2009, the Office of Policy and Management shall develop and operate a  
112 single, searchable web site accessible by the public at no cost to access  
113 which shall include:

114       (1) For each expenditure of state funds:

115       (A) The name of the principal location or residence of the recipient  
116 of the funds;

117       (B) The amount of the state funds expended;

118       (C) The type of transaction;

119       (D) The funding or expending agency;

120       (E) The budgetary source of the funds;

121       (F) A description of the purpose of the expenditure; and

122       (G) Any other relevant information specified by the Office of Policy  
123 and Management.

124       (2) The complete contents of the tax expenditure report published  
125 by the Department of Revenue Services.

126       (b) The web site established pursuant to this section shall include  
127 data for the fiscal year beginning July 1, 2008, and each fiscal year  
128 thereafter. Such data shall be available on such web site no later than  
129 thirty days after the last day of the preceding fiscal year.

130       (c) The Department of Revenue Services, the Treasurer and any  
131 other state agency shall provide to the Office of Policy and  
132 Management the information necessary to accomplish the purposes of  
133 this section.

134       (d) Nothing in this section shall be interpreted to require the  
135 disclosure of information considered confidential by state or federal  
136 law.

This act shall take effect as follows and shall amend the following sections:		
Section 1	<i>from passage</i>	New section
Sec. 2	<i>from passage</i>	New section
Sec. 3	<i>from passage</i>	New section
Sec. 4	<i>from passage</i>	New section

**Statement of Legislative Commissioners:**

In subsection (b) of section 1, "January 1, 2008" was changed to "July 1, 2008" for accuracy. In subparagraph (G) of subdivision (1) of subsection (a) of section 4, the "state Finance Office" was changed to the "Office of Policy and Management" for consistency.

**ET**            *Joint Favorable Subst.-LCO*

The following fiscal impact statement and bill analysis are prepared for the benefit of members of the General Assembly, solely for the purpose of information, summarization, and explanation, and do not represent the intent of the General Assembly or either chamber thereof for any purpose:

## OFA Fiscal Note

### State Impact:

Agency Affected	Fund-Effect	FY 09 \$	FY 10 \$
All	App Fund - Cost	Significant	Significant
Department of Information Technology	GF - Cost	4,200,000	2,900,000
Comptroller Misc. Accounts (Fringe Benefits) <sup>1</sup>	GF - Cost	700,000	1,400,000
Policy & Mgmt., Off.	GF - Cost	Significant	Significant

Note: App Fund=All Appropriated Funds; GF=General Fund

**Municipal Impact:** None

### Explanation

The cost to the Office of Policy and Management (OPM) to develop and implement an on-line accessible searchable state expenditure database is estimated to be more than \$1 million but anticipated to be less than \$5 million. The lower estimate is based on the initial costs involved in the development of a user-interface to access information already available within the Comptroller's CORE-CT system. Additional costs cannot be quantified until a plan has been developed.

The estimated cost to the Department of Information Technology (DOIT) to implement security plans specified in the bill is a one-time cost of \$1.3 million for computer equipment and related hardware in FY 09 and an on-going cost of \$2.9 million for personnel and office supplies in FY 09 and thereafter.

<sup>1</sup> The fringe benefit costs for state employees are budgeted centrally in the Miscellaneous Accounts administered by the Comptroller. The first year fringe benefit costs for new positions do not include pension costs. The estimated first year fringe benefit rate as a percentage of payroll is 25.36%. The state's pension contribution is based upon the prior year's certification by the actuary for the State Employees Retirement System (SERS). The SERS fringe benefit rate is 33.27%, which when combined with the rate for non-pension fringe benefits totals 58.63%.

The one-time cost in FY 09 is for the hardware necessary to implement the security plans specified in the bill. The on-going cost of \$2.9 million for FY 09 and after, includes \$2.7 million, excluding fringes, for 30 new positions at DOIT (3 IT Manager II, 1 Communications Officer, 25 Technical Analyst III, and 1 Technical Analyst I) and \$200,000 for software licenses, and office supplies for the Emergency Operations Center and the Test Lab. The associated fringe costs are \$700,000 in FY 09 and \$1.4 million in FY 10 and after to the Comptroller's Miscellaneous Account for Fringes.

The combined cost for agencies and quasi-public agencies to implement the security plans specified in the bill is estimated to cost between \$15.0 million and \$20.0 million in FY 09 and \$20.0 million and \$25.0 million in FY 10 and out years. The estimates assume that most agencies and quasi-public agencies will require at least one full-time Information Security Officer (EU-32) at an annual salary of \$90,000 plus fringes. Some agencies will require additional staff and resources whereas other agencies will not require any staffing and resources. Each agency will also require an additional \$100,000 annually to fund continuing improvements to data security systems in their control. There are currently 88 agencies and 11 quasi-public agencies.

It should be noted that the provisions in the bill do not specify what the security plans are supposed to be. Estimates for DOIT assume that they include the development and maintenance of Business Continuity (BC) and Disaster Recovery (DR) plans for all state agencies. This includes conducting Business Impact Analysis (BIA) for each agency and recoverability assessment (RA) for all platforms supporting applications. It also includes performing IT Security risk analyses for all state agencies to assess security of Network devices, Hosting platform, workstations and facilities. Expansion of Network Intrusion Prevention, establishment of an emergency operations center, development of security awareness programs and establishment of a disaster recovery test lab will also be required to meet provisions of the bill.

***The Out Years***

The annualized ongoing fiscal impact identified above would continue into the future subject to inflation.

---

**OLR Bill Analysis**

**sHB 5816**

***AN ACT CONCERNING INTERNET SECURITY.***

**SUMMARY:**

This bill requires, by January 1, 2009, the Office of Policy and Management (OPM) to develop and operate a single, searchable state expenditure website accessible by the public at no cost. The website must include data for the fiscal year beginning July 1, 2008 and subsequent fiscal years. The data must be available on the website within 30 days after the last day of the preceding fiscal year.

The bill requires the governor to appoint a chief information security officer and specifies the officer's duties. It requires each agency, by the start of each fiscal year, to develop an information security plan using the information security policies, standards, and guidelines the officer develops, and specifies the contents of the plans and the consequences if the plans are not developed on time. These can include suspending the agency's communications and information resources until the plan has been submitted and approved by the officer.

EFFECTIVE DATE: Upon passage

**STATE EXPENDITURE WEBSITE**

Under the bill, the website must cover the expenditure of all appropriated or non-appropriated funds by state entities. These include grants, contracts, subcontracts, tax refunds, rebates, or credits (other than those resulting from income tax overpayments), and expenditures pursuant to a compact between the governor and a federally recognized Indian tribe or nation in the state. On the other hand, these expenditure do not include transfers of funds between two

state agencies or payments of state or federal assistance to an individual.

The website must include, for each state expenditure:

1. the name of the principal location or residence of the recipient of the funds;
2. the amount of the state funds expended;
3. the type of transaction;
4. the funding or expending agency;
5. the budgetary source of the funds;
6. a description of the purpose of the expenditure; and
7. any other relevant information specified by the state "Finance Office" (presumably OPM).

The website must also contain the complete contents of the tax expenditure report published by the Department of Revenue Services (DRS). (In practice, the Office of Fiscal Analysis publishes the tax expenditure reports). It must include data for the fiscal year beginning January 1, 2008, and each fiscal year thereafter. The data must be available on such website no later than 30 days after the last day of the preceding fiscal year.

DRS, the treasurer, and any other state agency must provide OPM with the information needed to accomplish the purposes of these provisions. These provisions do not require the disclosure of information considered confidential by state or federal law.

#### **CHIEF INFORMATION SECURITY OFFICER**

The bill requires the governor to appoint a chief information security officer with experience in security and risk management for communications and information resources. Under the bill, "information security" means the protection of these resources from

unauthorized access, use, disclosure, disruption, modification, or destruction. The resources are (1) procedures, equipment, and software designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information; and (2) associated personnel, including consultants and contractors. The resources must be protected to (1) prevent improper information modification or destruction; (2) preserve authorized restrictions on information access and disclosure; (3) ensure timely and reliable access to and use of information; and (4) maintain the confidentiality, integrity, and availability of information.

The officer is responsible for:

1. developing and updating information security procedures, standards, and guidelines for all state agencies;
2. ensuring the incorporation of, and compliance with, information security policies, standards, and guidelines in the information security plans developed by state agencies under the bill;
3. directing information security audits and assessments in state agencies to ensure program compliance;
4. establishing and directing a risk management process to identify information security risks in state agencies and deploy risk mitigation strategies, processes, and procedures;
5. reviewing and approving state agency information security plans annually; and
6. conducting information security awareness training programs.

### **AGENCY INFORMATION SECURITY PLANS**

The bill requires each agency, by the start of each fiscal year, to develop an information security plan using the information security policies, standards, and guidelines developed by the officer. Agencies must submit the plans, by the start of each fiscal year, to the officer for

approval.

The plans must include periodic assessments of the risk and magnitude of the harm that could result from a “security incident.” Under the bill, a security incident is an accidental or deliberate event that results in or constitutes an imminent threat of the unauthorized access, loss, disclosure, modification, disruption, or destruction of communication and information resources. Each plan must also include:

1. a process for providing adequate information security for the communication and information resources of the state agency;
2. periodic security awareness training to inform the agency’s employees and users of its communication and information resources about information security risks and the responsibility of employees and users to comply with agency policies, standards, and procedures designed to reduce the risks;
3. periodic vulnerability assessment testing and evaluation of the effectiveness of information security for the state agency, which must be done at least annually;
4. a process for detecting, reporting, and responding to security incidents consistent with the information security standards, policies, and guidelines issued by the chief information security officer; and
5. plans and procedures to ensure the continuity of operations for information resources that support the operations and assets of the state agency during a security incident.

The plans may contain other elements and may provide for a phase-in for up to three years. Any plan providing for a phase-in period must include an implementation schedule for the period.

If an agency does not submit a plan to the officer by the start of the fiscal year or if the officer disapproves the plan, the officer must notify

the governor and the head of the agency. If no plan has been approved by October first of any year, the officer may suspend the operation of said agency's communication and information resources until the plan has been submitted to and approved by the officer.

By the beginning of each fiscal year, the head of each state agency must report to the chief information security officer on the development, implementation, and, if applicable, compliance with the phase-in schedule of the agency's security plan. By January 1, 2010, and annually thereafter, the officer must report to the governor and the Energy and Technology Committee concerning the implementation of the plans.

**COMMITTEE ACTION**

Energy and Technology Committee

Joint Favorable

Yea 21    Nay 0    (03/11/2008)