HOUSE BILL REPORT
HB 1008

As Reported by House Committee On:
General Government & Information Technology

Title: An act relating to authorizing the state auditor to conduct audits of state government and local agencies' data storage and management practices thereby protecting privacy and securing personal information from computer hacking or misuse of data.

Brief Description: Authorizing the state auditor to conduct audits of state government and local agencies' data storage and management practices thereby protecting privacy and securing personal information from computer hacking or misuse of data.

Sponsors: Representatives Smith, Hudgins, Hayes, Stanford, Moeller, Magendanz and Buys.

Brief History:
Committee Activity:
General Government & Information Technology: 1/30/15, 2/13/15 [DPS].

Brief Summary of Substitute Bill

- Authorizes the State Auditor to conduct audits of a state or local agency's data management and storage practices.
- Requires state agencies and local governments to report computer breaches to the State Auditor.

HOUSE COMMITTEE ON GENERAL GOVERNMENT & INFORMATION TECHNOLOGY

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 6 members: Representatives Hudgins, Chair; MacEwen, Ranking Minority Member; Caldier, Assistant Ranking Minority Member; McCabe, Morris and Takko.

Minority Report: Without recommendation. Signed by 1 member: Representative Senn, Vice Chair.

Staff: Marsha Reilly (786-7135).

Background:

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

The State Auditor (Auditor) is authorized to audit public accounts, investigate improper governmental activity, request prosecutions of wrongdoings, and report to the Director of the Office of Financial Management the names of persons who have received moneys belonging to the state that are not accounted for. The Auditor may also conduct independent, comprehensive performance audits of public agencies.

In December 2014 the Auditor released a report of a performance audit of the state's information technology security, including data security, network security, access security, application security, and operations management. The audit revealed that the agencies audited were not in full compliance with security standards.

Summary of Substitute Bill:

The Auditor is authorized, at his or her discretion, or when there is reasonable cause to believe that a misuse or inappropriate management of citizen data has occurred, to conduct an audit of a state or local agency's data management and storage practices. The requirement extends to nonprofit corporations that provide personal services to a state agency or to clients of a state agency.

Local governments must adopt standards consistent with the intended outcomes of those established by the Chief Information Officer, or generally accepted standards for information security, and establish a schedule to institute those standards. Effective July 1, 2018, the Auditor may begin audits of local governments to assess whether they are meeting the standards adopted for data management and storage practices.

The Auditor's Office must consult with the Office of the Chief Information Officer (OCIO) and local governments to provide training on information security for state and local governments. Audit results may only be provided to the state agency executive officer or local government executive body.

The Open Public Meetings Act is amended to allow a governing body to consider certain security information in executive session, including:

- infrastructure and security of computer and telecommunications networks;
- security and service recovery plans;
- security risk assessments and security test results to the extent vulnerabilities are identified; and
- other information that, if made public, may increase the risk to the confidentiality, integrity, or availability of agency security or to information technology infrastructure or assets.

Substitute Bill Compared to Original Bill:

The substitute bill added the following provisions:

- clarifies that the audits are to assess whether adopted standards for data management and storage practices are being met;

- requires state agencies and local governments to report computer breaches to the Auditor;
- verifies that audits of state agency data management and storage practices be conducted pursuant to the standards established by the chief information officer;
- requires local governments to establish standards and a schedule to implement those standards allowing time for procurement and training. Adopted standards must meet those established by the chief information officer, or other generally accepted standards for information security;
- specifies that audits of local governments' data management and storage practices may begin by July 1, 2018;
- requires the Auditor's Office to consult with the OCIO and local governments in providing training on information security for state and local governments. Requires that audit reports on data management and storage practices be provided only to state agency heads or executive bodies of local governments; and
- modifies the Open Public Meetings Act to require that discussions involving the security and vulnerability of information technology systems, plans, and assessments must be held during executive session.

Appropriation: None.

Fiscal Note: Available. New fiscal note requested on February 20, 2015.

Effective Date of Substitute Bill: The bill takes effect 90 days after adjournment of the session in which the bill is passed.

Staff Summary of Public Testimony:

(In support) The bill was brought forward as a way to assure cybersecurity and to protect individuals and the functions of government from cyberattacks. Cyberattacks are common and are sophisticated. The bill is not about someone's failure. The work of the OCIO and local governments is good, but the Auditor has a unique opportunity to look at these issues.

The Auditor audits over 2,000 local governments, and an audit to assess standards for data management and storage practices would be included as part of the accountability audits. The audits would focus on whether adopted standards are being met. This is a good risk management bill. Many local governments are not aware of the risks, and the bill will allow the Auditor to help local governments assess that risk. Risk-based assessments are a priority, and information technology risks are the highest risk.

An examination of data management practices and how agencies handle the records in their possession is very important. The bill might be improved by including data retrieval for public disclosure. Data retrieval is the primary method in which data is compromised.

(With concerns) The Chief Information Officer and the Consolidated Technology Services Agency support the bill but have concerns. The Association of Washington Cities (Cities) understands the intent of the bill, but has concerns. The Cities are not opposed to the concept

of security information and protecting privacy, but the bill does not do that. It does offer assistance to local governments in pointing out vulnerabilities. The Auditor now has the authority to conduct another audit. In addition to audits by the Auditor, local governments are also audited by insurance industries, banks, and many others. The Auditor should work with local governments to adopt standards before conducting an audit.

There are a number of Washington ports that have few staff members. It is important that the Auditor set standards and provide training before auditing.

This is an issue that local governments struggle with. The Auditor's Office is not the best entity for this audit as the Auditor has a policing function. Counties would like the training and resources in order to do what is needed.

(Opposed) None.

Persons Testifying: (In support) Representative Smith, prime sponsor; Matt Miller and Kelly Collins, State Auditor's Office; and Rowland Thompson, Allied Dailey Newspapers.

(With concerns) Michael Cockrill, Office of the Chief Information Officer; Rob St. John, Consolidated Technology Services; Victoria Lincoln, Association of Washington Cities; Ginger Eagle, Washington Ports Association; and Josh Weiss, Washington Association of Counties.

Persons Signed In To Testify But Not Testifying: None.