HOUSE BILL REPORT
ESSB 6528

As Passed House - Amended:
March 3, 2016

Title: An act relating to promoting economic development through protection of information technology resources.

Brief Description: Enacting the cybersecurity jobs act.

Sponsors: Senate Committee on Trade & Economic Development (originally sponsored by Senators Brown, Sheldon, Dammeier, Parlette, Schoesler, Warnick, Honeyford, Braun, Angel, Hewitt, Miloscia, O'Ban, Becker, Rivers and Rolfes).

Brief History:
Committee Activity:
Technology & Economic Development: 2/23/16, 2/26/16 [DPA];
General Government & Information Technology: 2/29/16 [DPA(GGIT w/o TED)].
Floor Activity:
Passed House - Amended: 3/3/16, 95-0.

Brief Summary of Engrossed Substitute Bill
(As Amended by House)

- Requires the Office of the Chief Information Officer (OCIO) to implement a process for detecting and responding to security incidents and to develop plans to ensure continuity of commerce in the event of a security incident.
- Requires the OCIO to work with stakeholders to develop a strategy that will make Washington a national leader in cybersecurity.
- Establishes performance metrics and requires the OCIO to report to the Legislature by December 1, 2020, on its achievement of these metrics.

HOUSE COMMITTEE ON TECHNOLOGY & ECONOMIC DEVELOPMENT

Majority Report: Do pass as amended. Signed by 11 members: Representatives Morris, Chair; Tarleton, Vice Chair; Smith, Ranking Minority Member; DeBolt, Assistant Ranking Minority Member; Fey, Hudgins, Magendanz, Nealey, Rossetti, Wylie and Young.

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.

Staff: Jasmine Vasavada (786-7301).

HOUSE COMMITTEE ON GENERAL GOVERNMENT & INFORMATION TECHNOLOGY

Majority Report: Do pass as amended by Committee on General Government & Information Technology and without amendment by Committee on Technology & Economic Development. Signed by 7 members: Representatives Hudgins, Chair; Kuderer, Vice Chair; MacEwen, Ranking Minority Member; Caldier, Assistant Ranking Minority Member; Johnson, Morris and Senn.

Staff: James Mackison (786-7104).

Background:

The Office of the Chief Information Officer.
The Office of the Chief Information Officer (OCIO) sits within the Consolidated Technology Services (CTS) Agency and is responsible for the preparation and implementation of a strategic information technology (IT) plan and enterprise architecture (EA) for the state. Led by the Chief Information Officer (CIO), the OCIO works toward standardization and consolidation of IT infrastructure, establishes standards and policies for EA, educates and informs the state on IT matters, evaluates current IT spending and budget requests, and oversees major IT projects, including procurements.

Consolidated Technology Services Agency.
In 2015 the Legislature consolidated functions of the OCIO, the CTS, and the enterprise applications division of the Department of Enterprise Services in a new executive branch agency, legally known as the CTS Agency and branded to the public in certain contexts as "WaTech."

Summary of Amended Bill:

Duties of the Office of the Chief Information Officer.
The OCIO must implement a process for detecting and responding to security incidents consistent with information security standards, policies, and guidelines adopted by the CIO. "Security incident" means an accidental or deliberate event that results in unauthorized access, loss, disruption, or destruction of communication and IT resources. "Information security" means the protection of communication and information resources from unauthorized access, use, disclosure, disruption, modification, or destruction in order to prevent improper information modification or destruction, preserve authorized restrictions on information access and disclosure, ensure timely and reliable access to and use of information, and maintain the confidentiality, integrity, and availability of information.

The OCIO must develop plans and procedures to ensure the continuity of operations for IT resources in the event of a security incident. The OCIO must work with the Department of Commerce and other economic development stakeholders to facilitate the development of a strategy that includes key local, state, and federal assets that will make Washington a national leader in cybersecurity. The OCIO must collaborate with community colleges, universities,

the National Guard, the Department of Defense, the Department of Energy, and national laboratories to develop the strategy.

Performance Metrics.
The OCIO must evaluate the state's performance in achieving leadership in cybersecurity, by measuring and reporting to the Legislature by December 1, 2020, on the extent to which the state has achieved the following objectives, as measured by the following metrics: high levels of compliance with the state's IT security policy and standards; recognition from the federal government; development of future leaders in cybersecurity; and broad participation in cybersecurity training and exercises or outreach.

Title.
The act may be known and cited as the Cybersecurity Jobs Act of 2016.

Appropriation: None.

Fiscal Note: Available.

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

Staff Summary of Public Testimony (Technology & Economic Development):

(In support) News of cyberattacks is increasing and makes citizens nervous about the safety of personal and private information. The state must grow its own leaders in cybersecurity and educate children so that they will want to earn a degree in this field. These jobs are high-paying, some starting at more than $100,000 a year. Washington is a leader. Many regional activities are occurring here, including research and development, private cyber assessments, and workforce development. This bill brings together stakeholders, including the national laboratories, universities, and community colleges. There are clear national standards, best practices, and management controls the state can benchmark its performance against.

(Opposed) None.

Staff Summary of Public Testimony (General Government & Information Technology):

(In support) The bill takes what is already being done and puts it into law. The Chief Information Security Officer is responsible for actions required in the bill. Requiring metrics, as is done in the amendment, is good public policy. Input was provided on the definitions within the bill. The committee and sponsors are commended for focusing on this issue on behalf of citizens and those involved in cybersecurity.

(Opposed) None.

Persons Testifying (Technology & Economic Development): Senator Brown, prime sponsor; Jim Jesernig and Ann Lesperance, Battelle; and Michael Cockrill and Agnes Kirk, Washington Technology Solutions.

Persons Testifying (General Government & Information Technology): Michael Cockrill and Agnes Kirk, Washington Technology Solutions.

Persons Signed In To Testify But Not Testifying (Technology & Economic Development): None.

Persons Signed In To Testify But Not Testifying (General Government & Information Technology): None.