

---

## Technology & Economic Development Committee

---

### ESSB 6528

**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 Summary of Engrossed Substitute Bill

- Requires the Office of the Chief Information Officer (OCIO) to implement a process for detecting and responding to security incidents.
- Requires the OCIO to develop plans to ensure continuity of commerce in the event of a security incident.
- Requires the OCIO to work with stakeholders, including the Department of Commerce, to develop a strategy that will make Washington a national leader in cybersecurity.

**Hearing Date:** 2/23/16

**Staff:** Jasmine Vasavada (786-7301).

#### **Background:**

##### The Office of the Chief Information Officer.

The Office of the Chief Information Officer (OCIO) sits within the Office of Financial Management (OFM) 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.

---

*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.*

Consolidated Technology Services Agency.

In 2015 the Legislature consolidated functions of the OCIO, Consolidated Technology Services (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 Bill:**

Duties of the OCIO.

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.

Placement of the OCIO.

The OCIO is placed within Washington Technology Solutions, rather than within the CTS Agency.

Title.

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

**Appropriation:** None.

**Fiscal Note:** Available.

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