SENATE BILL REPORT
2SHB 1929

As Reported by Senate Committee On:
State Government, March 29, 2017

Title: An act relating to building a more robust state information technology security posture by leveraging assets at the military department and other agencies responsible for information technology systems and infrastructure.

Brief Description: Concerning independent security testing of state agencies' information technology systems and infrastructure by the military department.

Sponsors: House Committee on Appropriations (originally sponsored by Representatives Hudgins, Harmsworth and Tarleton).

Brief History: Passed House: 3/06/17, 98-0.
Committee Activity: State Government: 3/15/17, 3/29/17 [DP-WM].

Brief Summary of Bill

- Authorizes the Office of the Chief Information Officer (OCIO) to test the security vulnerabilities of state agency information technology (IT) systems.
- Authorizes the Military Department to test, upon request of any local government or private entity, the security of the entities' critical infrastructure.
- Requires the Chief Information Security Officer, Utilities and Transportation Commission (UTC), and Military Department to meet regularly regarding IT systems & infrastructure security.

SENATE COMMITTEE ON STATE GOVERNMENT

Majority Report: Do pass and be referred to Committee on Ways & Means.
Signed by Senators Miloscia, Chair; Zeiger, Vice Chair; Hunt, Ranking Minority Member; Kuderer and Pearson.

Staff: Melissa Van Gorkom (786-7491)

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.

Background: Office of the Chief Information Officer. The Legislature established the OCIO within the Consolidated Technology Services agency, most commonly referred to as WaTech in 2011. The OCIO prepares a state strategic IT plan that includes a statewide mission, goals, and objectives for the use of IT, including security standards and policies to protect the information processed in the state IT system. All state agencies are required to review and update IT security programs and certify compliance with the state IT standards established by the OCIO annually and obtain an independent compliance audit every three years.

Military Department. The Military Department administers the state's emergency management program. The Adjutant General, Director of the Military Department, serves as the Homeland Security Advisor (HSA) for significant incidents in the state of Washington and reports directly to the Governor regarding these incidents. In 2015, the Governor designated the HSA as the senior official for a response to a significant cyber security incident both in the state and at the federal level and designated the Military Department as the primary agency for external communication with the Department of Homeland Security for significant cyber security incident exercises.

Summary of Bill: OCIO is authorized to test the security vulnerability of any state agency's IT systems, coordinating with the agency if necessary to ensure business operations are not disrupted, and must share the test results with the agency. Testing of institutions of higher education, the judiciary, and Legislature may only be conducted at their request.

The Military Department may conduct independent security testing of any local government or private entity involved in critical infrastructure management, upon the request of the governmental or private entity. Critical infrastructure includes systems or assets vital to the national security, economy, and public health and safety.

The testing agency may assist the entity tested in addressing any vulnerabilities identified in the test.

The Chief Information Security Officer, UTC, and Military Department must meet regularly to share information, trends, and best practices regarding IT systems and infrastructure security.

If funding is not provided by June 30, 2017, this act is null and void.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: No.

Effective Date: Ninety days after adjournment of session in which bill is passed.

Staff Summary of Public Testimony: PRO: In 2015, at the request of Snohomish PUD, the National Guard conducted a pilot project on our utility system which was quite informative

and valuable in helping the agency shore up any vulnerabilities. This bill would provide a process and assistance to other local governments which would be helpful.

OTHER: Washington National Guard employs more than 600 cyber security professionals to help conduct vulnerability assessments on critical infrastructures in Washington. The private sector owns 85 percent of Washington's critical infrastructure, and the Military Department can assist in advising and training these entities. The Military Department would do tests upon request, contracting with those entities to preform those tests and would be reimbursed for their services.

Persons Testifying: PRO: Dave Arbaugh, Snohomish PUD.

OTHER: Colonel Ken Borchers, Deputy Commander, 252nd Operations Group, Washington Air National Guard.

Persons Signed In To Testify But Not Testifying: No one.