HOUSE BILL REPORT
HB 1929

As Reported by House Committee On:
State Government, Elections & Information Technology

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: Representatives Hudgins, Harmsworth and Tarleton.

Brief History:
Committee Activity:
State Government, Elections & Information Technology: 2/14/17, 2/15/17 [DPS].

Brief Summary of Substitute Bill

- Directs the Consolidated Technology Services agency to test the security vulnerabilities of state agency information technology systems.
- Authorizes the Military Department to test, upon request of any local government or private entity, the security of the entities' critical infrastructure.

HOUSE COMMITTEE ON STATE GOVERNMENT, ELECTIONS & INFORMATION TECHNOLOGY

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 9 members: Representatives Hudgins, Chair; Dolan, Vice Chair; Koster, Ranking Minority Member; Volz, Assistant Ranking Minority Member; Appleton, Gregerson, Irwin, Kraft and Pellicciotti.

Staff: Sean Flynn (786-7124).

Background:

State Cybersecurity Programs.

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. In 2011 the Consolidated Technology Services (CTS) agency was created as part of a reorganization of state government information technology (IT) infrastructure functions and services. The CTS provides information services to public agencies, operates the state data center, and offers IT services, including data security and storage. In 2015 the CTS also assumed IT functions from the Department of Enterprise Services.

In 2015 the Legislature also directed the CTS to establish statewide security standards and policies to protect the information processed in the state IT systems, and appoint a state chief information security officer. All state agencies were directed to develop an IT security program in accordance with the state standards established by the CTS. Each agency must certify its compliance with the state security standards, and must obtain an independent compliance audit every three years.

The Military Department. The Military Department administers the state's comprehensive program of emergency management. The Adjutant General, acting as Director of the Military Department, is responsible for directing and coordinating the state preparation, response, and recovery from emergencies and disasters.

In 2013 Governor Inslee designated the Military Department as the primary agency for external communication with the federal Department of Homeland Security for all cybersecurity matters within state government. The Governor appointed the Adjutant General as the senior official representing Washington for management and coordination of cybersecurity issues within the state and at the federal level.

Summary of Substitute Bill:

The CTS is authorized to test the security vulnerability of any state agency's IT systems, without disrupting the agency's business operations. The test results must be shared with the agency and the CTS may assist the agency in addressing any vulnerabilities identified in the test.

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 Military Department may assist the entity in addressing any vulnerabilities identified in the test. The Military Department, chief information security officer, and the Utilities and Transportation Commission must meet regularly to discuss best practices and trends regarding IT systems security testing.

Substitute Bill Compared to Original Bill:

The requirement for the Military Department to share test results with the chief information security officer and the Utilities and Transportation Commission is removed, and those entities must meet regularly to discuss best practices and trends.

Appropriation: None.

Fiscal Note: Available.

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) None.

(Opposed) None.

(Other) The Military Department has considerable cybersecurity capabilities that can be used by the private entities that hold significant sensitive information. The Military Department uses memoranda of understanding with private entities to test the vulnerabilities of private systems. The information gathered through IT systems security testing is very sensitive. It is important that the such information is not shared with other entities.

Persons Testifying: Ken Borchers, Washington National Guard; and Dave Arbaugh, Snohomish Public Utility District.

Persons Signed In To Testify But Not Testifying: None.