Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

State Government, Elections & Information Technology Committee

HB 2172

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

Sponsors: Representative Hudgins.

Brief Summary of Bill

- Allows the Office of the State Chief Information Officer within the Consolidated Technology Services Agency to conduct testing on the security of any state agency's information technology system.
- Allows the Military Department to conduct testing, upon request, on the security of the information technology system of any private entity or unit of local government that is involved in the management of critical infrastructure.

Hearing Date: 1/19/18

Staff: Travis Yonker (786-7383).

Background:

In 2011 the Legislature created the Consolidated Technology Services Agency, which became known as WaTech, to establish a centralized information technology organization to assist state government agencies, institutions of higher education, the Legislature, and the Judiciary in their information technology practices. The Legislature also created the Office of the State Chief Information Officer (OCIO) within WaTech to establish standards and policies for operation of information technology services throughout state government.

As part of the OCIO's duties, it must establish security standards and policies to ensure the confidentiality, availability, and integrity of the information transacted, stored, or processed in the state's information technology systems and infrastructures.

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.

All state agencies must develop an information technology security program that adheres to the OCIO's security standards and policies, While institutions of higher education, the Legislature, and the Judiciary must develop an information technology security program that is comparable to the intended outcomes of the OCIO's security standards and policies.

Summary of Bill:

The security of any state agency's information technology systems and infrastructure may be tested by the OCIO to identify and mitigate system vulnerabilities, subject to the following requirements:

- the test must apply framework from the cybersecurity excellence assessment criteria or similar objective criteria to give measurable results for the test;
- the OCIO must coordinate with the state agency being tested to minimize disruptions; and
- the results of the test must be shared with the state agency tested and with legislators upon request.

Cybersecurity excellence assessment is an assessment of cybersecurity operational performance using a framework approved by the National Institute of Standards and Technology, a part of the United States (U.S.) Department of Commerce.

State agencies may be assisted by the OCIO in the remediation of any vulnerabilities identified by the test, however the OCIO may only test the Judiciary or the Legislature at that organization's request. For testing to occur with the Legislature, the OCIO must develop procedures with the Legislature, including enforceable nondisclosure agreements, to ensure that such testing does not interfere to perform its constitutional duties.

Upon request, the Military Department may conduct independent security tests of the information security of any private entity or unit of local government in Washington that is involved in the management of critical infrastructure, which means systems and assets, managed by private entities or local governments, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, economic security, or public health or safety. The Military Department may assist in the remediation of any vulnerabilities identified by such a test.

The Chief Information Security Officer of the OCIO, the Utilities and Transportation Commission, and the Military Department must meet regularly to share information, trends, and best practices related to information technology systems and infrastructure security.

Appropriation: None.

Fiscal Note: Available.

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