

HOUSE BILL REPORT

HB 1470

As Reported by House Committee On:
General Government & Information Technology

Title: An act relating to establishing a blue-ribbon panel on cybersecurity.

Brief Description: Establishing a blue-ribbon panel on cybersecurity.

Sponsors: Representatives Hudgins, Smith, Stanford, S. Hunt, Ormsby, McBride and Tarleton.

Brief History:

Committee Activity:

General Government & Information Technology: 1/30/15, 2/6/15 [DPS].

Brief Summary of Substitute Bill

- Directs the Office of the Chief Information Officer (OCIO) to convene a blue-ribbon panel focused on local government cybersecurity issues, co-chaired by the Chief Information Officer and the Director of the Military Department.
- Requires the OCIO to submit a report detailing the recommendations of the panel by December 2016.

HOUSE COMMITTEE ON GENERAL GOVERNMENT & INFORMATION TECHNOLOGY

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 7 members: Representatives Hudgins, Chair; Senn, Vice Chair; MacEwen, Ranking Minority Member; Caldier, Assistant Ranking Minority Member; McCabe, Morris and Takko.

Staff: Derek Rutter (786-7157).

Background:

Office of the Chief Information Officer.

The Office of the Chief Information Officer (OCIO) was created in 2011 within the Office of Financial Management (OFM). The OCIO is responsible for the preparation and implementation of a strategic information technology (IT) plan and enterprise architecture for

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.

the state. The OCIO works toward standardization and consolidation of IT infrastructure and establishes IT standards and policies, including state IT security policies. The OCIO also prepares a biennial state performance report on IT, evaluates current IT spending and budget requests, and oversees major IT projects.

Military Department.

The Military Department administers the state's comprehensive program of emergency management. The Adjutant General, who is the Director of the Military Department, is responsible for developing a comprehensive, all-hazard emergency plan for the state that includes an analysis of natural, technological, or human-caused hazards, and procedures to coordinate local and state resources in responding to such hazards.

In 2013 Governor Inslee designated the Military Department as the primary agency for external communication with the Department of Homeland Security for all cybersecurity matters within state government and 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 Office of the Chief Information Officer (OCIO) shall convene a blue-ribbon panel on cybersecurity that will review issues such as protecting critical infrastructure from the threat of cyberattack, protecting data transfer and enhancing the security of the state's intergovernmental network, and best practices for local government response in the event of a cybersecurity incident. The Chief Information Officer and the Director of the Military Department will be co-chairs of the panel. The OCIO will provide staff support for the panel. The panel must publish its meeting schedule, and the OCIO must submit a report of the panel's recommendations to the legislature, the governor, and organizations representing local governments or utilities, by December 12, 2016.

Substitute Bill Compared to Original Bill:

The substitute bill specifies that the panel will be co-chaired by the Chief Information Officer and the Director of the Military Department. "Protecting data transfer" is added to the list of issues to be considered by the panel. The panel's reporting deadline is moved from December 12, 2015, to December 12, 2016.

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) Cybersecurity is a huge issue; cybersecurity incidents cost 2 percent of gross domestic product according to some statistics. The dangers of government-to-government "cyber war," as well as threats from rogue and criminal hacker groups, are underestimated. Local governments appreciate that the state, with this bill, wants to provide help and support on this issue.

(Opposed) None.

Persons Testifying: Lew McMurrin; and Josh Weiss, Washington State Association of Counties.

Persons Signed In To Testify But Not Testifying: None.