Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

State Government & Tribal Relations Committee

HB 2044

Brief Description: Concerning the protection of critical constituent and state operational data against the financial and personal harm caused by ransomware and other malicious cyber activities.

Sponsors: Representatives Boehnke, Hackney, Fitzgibbon, Kloba, Ormsby, Sutherland, Ramel and Young.

Brief Summary of Bill

- Requires the Office of the Chief Information Officer (OCIO) to design, develop, and implement enterprise technology standards (standards) specific to malware and ransomware protection, backup, and recovery.
- Requires the OCIO to establish a ransomware education and outreach program to educate employees of public agencies on the prevention, response, and remediation of ransomware.
- Requires certain state agencies to comply with the standards established by the OCIO unless a waiver is approved.
- Requires various reporting by the OCIO on information relating to mission critical applications, business essential applications, the status of immutable backups for each application, and the breadth of threat landscape.

Hearing Date: 1/31/22

Staff: Desiree Omli (786-7105).

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not part of the legislation nor does it constitute a statement of legislative intent.

Background:

Consolidated Technology Services.
The Consolidated Technology Services agency, also known as the Washington Technology Solutions (WaTech), supports state agencies as a centralized provider and procurer of certain information technology (IT) services. The Office of the Chief Information Officer (OCIO) is established within WaTech and has certain primary duties related to state government IT, which include establishing statewide enterprise architecture for IT and standards for consistent and efficient operation of IT services throughout state government. The OCIO is responsible for establishing security standards and policies to ensure the confidentiality and integrity of information transacted, stored, or processed in the state's IT systems and infrastructure. In 2021 the Office of Cybersecurity (OCS) was statutorily established within the OCIO. Some of the OCS's responsibilities include establishing standards and policies to protect the state's information technology systems and infrastructure, developing a centralized cybersecurity protocol for protecting and managing state IT assets and infrastructure, creating a model incident response plan for agencies to adopt for certain incidents, and defining core services that are required to be managed by agency IT security programs.

Under the OCIO policy, agencies must classify data into categories based on the sensitivity of the data as follows: (Category 1) public information; (Category 2) sensitive information; (Category 3) confidential information that is specifically protected from release or disclosure by law, such as certain personal information, certain information about public employees, lists of individuals for commercial purposes, and information about the infrastructure and security of computer and telecommunication networks; and (Category 4) confidential information that is specifically protected from disclosure by law and for which especially strict handling requirements are dictated and the disclosure of which may result in serious consequence from unauthorized disclosure such as threats to health and safety or legal sanctions.

Public Records Act.
The Public Records Act (PRA) requires state and local agencies to make all public records available for public inspection and copying unless a record falls within an exemption under the PRA or another statute that exempts or prohibits disclosure of specific information or records. The PRA is liberally construed, and its exemptions interpreted narrowly. To the extent necessary to prevent an unreasonable invasion of personal privacy, an agency must delete identifying details from the records sought when it makes a record available. A person's right to privacy is violated only if disclosure would be highly offensive to a reasonable person and is not of legitimate concern to the public. Exemptions under the PRA are permissive, meaning that an agency, although not required to disclose, has the discretion to provide an exempt record. Certain information relating to security is exempt from disclosure under the PRA. For example, information regarding the public and private infrastructure and security of computer and telecommunications networks are exempt. Public and private infrastructure and security of computer and telecommunications networks includes: security passwords; security access codes and programs; security risk assessments; security test results to the extent that they identify specific system vulnerabilities; and any other information which, if released, may increase the

risk to the confidentiality, integrity, or availability or security of IT infrastructure or assets.

Summary of Bill:

The OCIO must design, develop, and implement enterprise technology standards (standards) specific to malware and ransomware protection, backup, and recovery. The standards must be reviewed annually.

The OCIO must also establish a ransomware education and outreach program to educate public agency employees on prevention, response, and remediation of ransomware. As part of the education program, the OCIO must publish and distribute ransomware-response educational materials specifically for certain chief financial and chief information officers of state agencies. In addition, the OCIO must modify existing portfolio reporting mechanisms to support the collection of data necessary to monitor risk associated with malware and ransomware protections, and identify a list of mission critical applications that need additional protections.

Certain requirements are established for technology projects. Ransomware protection, data security, and continuity of operations are considered critical success factors of state-managed technology projects. Projects submitted for risk assessment must include the agency's intent to incorporate data backup and recovery for the purpose of data security and continuity of operations. In addition, technology budgets must include separate line items for backup and recovery services. Each project must include confirmation of an immutable backup solution and a successful test of application and data recovery. "Immutable backup" means that no external or internal operation can modify the data and the data must never be available in a read or write state to the client.

Except for institutions of higher education, a state agency that is defined within the standards established by the OCIO must:

- comply with the standards implemented by the OCIO;
- execute and analyze monthly vulnerability scans and make data available to certain entities upon request;
- ensure that all mission critical applications, business essential applications and other data that requires special handling is protected;
- perform an assessment of their applications and resources containing data and report the size of managed data to the OCIO;
- provide the OCIO, by September 1, 2022, with a confidential list of prioritized applications based on mission criticality and impact to constituents in the event of system failure or data loss; and
- ensure that all mission critical applications, business essential applications, and other resources containing Category 3 or 4 data are protected in accordance with the established standards.

An agency may obtain a waiver from the OCIO exempting it from compliance with the standards. Waivers are approved based on a written business justification from the requesting

agency, and it must be signed by the chief executive, chief financial officer, and risk manager of the requesting agency. The waiver and any data used to inform the waiver are exempt from public disclosure.

By October 31, 2023, the OCIO must analyze and aggregate the data reported by state agencies and report the following to the Governor and Legislature:

- information regarding mission critical applications and business essential applications, such as the total number of each application, the amount of data associated with each application, the estimated annual data change and growth rates for each application, the percent of each application with immutable backups, the percentage of each application that undergoes annual continuity of operations exercises, and the percentage each application that meets the established standards;
- the percentage of applications with cataloged and categorized data;
- a list of state agencies that have received a waiver;
- prioritized applications identified by each state agency; and
- recommendations for further legislation, rules, and policy to increase protections against ransomware.

The report issued by the OCIO and information used to inform the report are confidential and may not be disclosed.

By December 31, 2025, the Office of Financial Management, Department of Enterprise Services, and WaTech must ensure that all mission critical and business essential IT systems are compliant with established standards and supported by immutable backups.

Beginning on December 31, 2024, the OCIO must submit a biannual report to the Legislature, Governor, and Technology Services Board on:

- the number of mission critical applications and business essential applications, and the amount of each with immutable backups;
- the number of business essential applications with standard-compliant backups;
- the number of applications containing Category 3 or 4 data, and the amount with immutable backups;
- the breadth of threat landscape;
- a prioritized list of systems requiring immutable backups and the cost of implementing immutable backups for each;
- the number of staff required to manage malware prevention and response;
- progress toward protection; and
- recommendations for additional work to protect critical state IT systems.

The biannual report is exempt from public disclosure.

The Information Security Account is created in the State Treasury as an appropriated account. Expenditures may only be used to protect critical state agency IT systems for which data backup and recovery are essential.

The OCIO must apply for any federal grants or other financial assistance program for the purpose of security and protection to critical state agency IT systems.

The act is known as the Washington State Ransomware Protection Act.

Appropriation: $5,000,000 from the State General Fund.

Fiscal Note: Preliminary fiscal note available.

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