HOUSE BILL REPORT
HB 2044

As Reported by House Committee On:
State Government & Tribal Relations

Title: An act relating to the protection of critical constituent and state operational data against the financial and personal harm caused by ransomware and other malicious cyber activities.

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 History:
Committee Activity:
State Government & Tribal Relations: 1/31/22, 2/2/22 [DPS].

Brief Summary of Substitute Bill

- Requires the Office of the Chief Information Officer (OCIO) to design, develop, and implement enterprise technology standards for 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 perform an assessment of their applications and resources containing data and provide the OCIO with a confidential list of prioritized applications based on mission criticality and impact to constituents in the event of system failure or data loss.
- 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.

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.

HOUSE COMMITTEE ON STATE GOVERNMENT & TRIBAL RELATIONS

Majority Report: The substitute bill be substituted therefor and the substitute bill do pass. Signed by 7 members: Representatives Valdez, Chair; Lekanoff, Vice Chair; Volz, Ranking Minority Member; Walsh, Assistant Ranking Minority Member; Dolan, Graham and Gregerson.

Staff: Desiree Omli (786-7105).

Background:

Consolidated Technology Services.
The Consolidated Technology Services agency, also known as 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: for public information;
- Category 2: for sensitive information;
- Category 3: for 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: for 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 Substitute Bill:

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

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 chief financial and chief information officers of state agencies. In addition, the OCIO must provide ongoing assistance to the Legislature by identifying mission critical systems that do not maintain backup and recovery capabilities and may require further investment to do so. The OCIO must modify existing portfolio reporting mechanisms to support the collection of data necessary to monitor risk associated with malware and ransomware protections.

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

- 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 30, 2022, with a confidential list of prioritized applications based on mission criticality and impact to constituents in the event of a 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.

The data reported by agencies must be analyzed for risk and used to provide the Legislature with a prioritized list of mission critical systems that requires additional protections to maintain continuity of operations in the event of malicious cyber activity.

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.

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

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.

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. "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.

The Information Security Account is created in the custody of the State Treasurer as a non-appropriated account. Disbursements from the account are subject to authorization by the Director of WaTech (Director). Expenditures from the account may only be used for state agencies to procure immutable data backup and disaster recovery services for mission critical and business essential applications or other critical IT systems. The Director must consider disbursements based on the agency's prioritized application list to ensure the funding is allocated to protect the most vulnerable IT systems containing the most sensitive public information. Money in the account may supplant existing funding to WaTech.

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

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

Substitute Bill Compared to Original Bill:

The requirements that the OCIO design and implement standards specifically for incident reporting and incident response management and remediation and annually review the standards are removed.

The requirement that state agencies comply with the standards is removed, which also removes provisions relating to the waiver from compliance with the standards. The requirement that state agencies execute and analyze monthly vulnerability scans is removed.

The date for state agencies to submit to WaTech a confidential list of prioritized applications based on mission criticality and impact to constituents in the event of system failure or data loss is moved from September 1, 2022, to September 30, 2022.

The OCIO is required to provide ongoing assistance to the Legislature by identifying mission critical systems that do not maintain backup and recovery capabilities.

The purpose of analyzing data that baselines and monitors risk associated with malware and ransomware protections is clarified to require that the data reported by agencies must be analyzed by the OCIO for risk and used to provide the Legislature with a prioritized list of mission critical systems that require additional protections to maintain continuity of operations in the event of malicious cyber activity.

The requirement for technology projects submitted for risk assessment to include an indication of the agency's intent to incorporate data backup and recovery into the project scope is removed.

The Information Technology Security Account is changed from an appropriated to a non-appropriated account and makes the account subject to disbursements by the Director to state agencies to procure immutable data backup and disaster recovery services. WaTech's

decisions to disburse funds must consider the agency's prioritized application list. Money in the account may supplant existing funding to WaTech.

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

Fiscal Note: Preliminary fiscal note available. New fiscal note requested on February 2, 2022.

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) The State Auditor's report published in 2020 highlighted glaring gaps in the state agency's ability to protect public data. As we moved online as a result of COVID-19, public and private data were put at a higher risk due to increased dependency on technology. Malicious cyber activity has increased by 600 percent since 2018. Data backup and investing in recovery systems are ways to protect against ransomware attacks. As demonstrated by the ransomware attack on Lincoln County during the certification of the election in 2020, bad actors are after the valuable identifying information that state agencies collect such as a person's signature, name, address, and date of birth. A person who has access to this information can download another person's ballot online and print a fraudulent ballot, which, if received first, is treated as a legitimate ballot.

Most agency applications used do not have a data backup systems. Mission critical and business essential applications are what we want to protect first. Immutable backups will make it so the data is not changed when it's stored and will allow agencies to recover the data unchanged from those who hold it hostage. This policy signifies that the state will continue its commitment to good stewardship of its residents data and fight against cyber attacks.

(Opposed) None.

(Other) Small and medium sized organizations like state agencies are disproportionately impacted by cyber attacks. Ransomware is overwhelming all organizations. An attack occurs every 11 seconds and the number is growing. The global cost of cyber attacks was around $17 billion in 2020 alone. After an attack, full recovery of data can take six to nine months if there is no backup.

The use of data backup systems and disaster recovery is an important component of recovery from cyber attacks, but there are other security controls that are also important for proactive ransomware protection. WaTech has adopted a cloud-first policy with an intent to migrate state technology assets to cloud services. For applications that aren't cloud ready,

they may need to seek data backup services within the state's data center to comply with the 2025 deadline in the bill.

Persons Testifying: (In support) Representative Matt Boehnke, prime sponsor; and Tamborine Borrelli, Washington Election Integrity Coalition United.

(Other) Jerry Cochran, Pacific Northwest National Lab; and Derek Puckett, Washington Technology Solutions.

Persons Signed In To Testify But Not Testifying: None.