Washington State
House of Representatives
Office of Program Research

BILL ANALYSIS

State Government & Tribal Relations Committee

ESSB 5432

Brief Description: Concerning cybersecurity and data sharing in Washington state government.

Sponsors: Senate Committee on Environment, Energy & Technology (originally sponsored by Senators Carlyle, Nguyen, Conway, Das, Dhingra, Keiser, Liias, Nobles and Randall; by request of Office of the Governor).

Brief Summary of Engrossed Substitute Bill

- Creates the Office of Cybersecurity (OCS) within the Office of the Chief Information Officer (OCIO) and transfers the OCIO's responsibilities relating to state information technology (IT) security programs to the OCS.
- Requires the OCS to collaborate with state agencies to develop a catalog of cybersecurity services and functions for the OCS to perform.
- Requires the Office of Financial Management to contract with an independent third party to audit the security and protection of digital assets to test and assess the state's overall security posture.
- Sets standards for data sharing and major cybersecurity incident reporting.

Hearing Date: 3/10/21

Staff: Desiree Omli (786-7105).

Background:

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.

The Consolidated Technology Services Agency.

General. 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 Director of WaTech is the state Chief Information Officer (CIO).

Office of the Chief Information Officer. The Office of the Chief Information Officer (OCIO) is statutorily 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 also establishes security standards and policies to ensure the confidentiality and integrity of information transacted, stored, or processed in the state's IT systems and infrastructure.

Under OCIO-issued 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.
- Category 4: Confidential information requiring special handling.

Office of Cybersecurity. The Office of Cybersecurity (OCS) is housed within WaTech but is not statutorily created. The OCIO is, however, statutorily required to appoint a state Chief Information Security Officer (CISO). The CISO leads the existing OCS, which provides strategic direction for cybersecurity and protects the state government network from growing cyber threats. The OCS also detects, blocks, and responds to cyberattacks on state networks, and helps prevent and mitigate threats.

Office of Privacy and Data Protection. The Office of Privacy and Data Protection (OPDP) is statutorily created within the OCIO and serves as a central point of contact for state agencies on policy matters involving data privacy and data protection. The primary duties of the OPDP with respect to state agencies include conducting privacy reviews and trainings, coordinating data protection, articulating privacy principles and best policies, and working with the CIO in the review of major state agency projects involving personally identifiable information.

State Information Technology Security Programs.

Each state agency, institution of higher education, the Legislature, and the judiciary must develop an IT security program. The IT security programs developed by institutions of higher education, the Legislature, and the judiciary, must be comparable to the intended outcomes of the OCIO's security standards and policies.

State agencies are subject to additional statutory requirements. Each state agency must annually review and update its IT security program and certify to the OCIO that its program is compliant with the OCIO's security standards and policies. The OCIO must require state agencies to obtain an independent compliance audit of its IT security program and controls once every three years.

The purpose of the audit is to determine whether the agency's IT security program is compliant with the standards and polices established by the agency, and that security controls are operating efficiently.

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.

Federal Cybersecurity Framework.
Federal Executive Order 13636 directed the National Institute of Standards and Technology (NIST) to develop a voluntary framework for reducing cyber risks to critical infrastructure. The cybersecurity framework developed by the NIST is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk.

Summary of Engrossed Substitute Bill:

Office of Cybersecurity.
Creation and Principle Responsibilities. The OCS is statutorily created within the OCIO. The CIO appoints the CISO who will act as the director of the OCS. The CISO or his or her designee serves as the state's point of contact for all major cybersecurity incidents.

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, and providing formal guidance to agencies on practices and standards to ensure a whole government approach to cybersecurity;
- detecting and responding to security incidents;

- creating a model incident response plan for agencies to adopt for certain incidents;
- ensuring the continuity of state business in the event of a security incident;
- defining core services that are required to be managed by agency IT security programs; and
- developing a process for reviewing and evaluating agency proposals for additional cybersecurity services to ensure alignment with enterprise IT security strategy.

In carrying out these duties, the OCS must use or rely on industry standards and widely adopted cybersecurity standards with a preference for United States federal standards.

Catalog of Services. The OCS must collaborate with state agencies to develop a catalog of cybersecurity services and functions for the OCS to perform. By July 1, 2022, the OCS must report to the Legislature and the Governor on cybersecurity services and functions that should be performed by the OCS, core capabilities of the OCS, security functions which should remain within agency IT security programs, a model for accountability of agency security programs, and services and functions required to protect confidential information that is specifically protected from disclosure by state or federal law. The OCS must update and publish its catalog of services and performance metrics on a biennial basis.

State Information Technology Security Programs.
Transfer of OCIO Responsibilities. With respect to state IT security programs, the OCIO's oversight and statutory responsibilities are transferred to the new OCS. Information technology security program standards and polices are now set by the OCS, and any IT security program required to be developed must be comparable to the intended outcomes of the OCS's standards and policies, or, in the case of state agencies, compliant with the OCS's standards and policies. An additional requirement is imposed on state agencies to provide the OCS with a list of business needs and agency program metrics.

Reporting of Agency Review and Audit Findings. In the event that an agency review or audit identifies any failure to comply with the standards and policies of the OCS or identifies any material cybersecurity risk, the OCS must require the agency to develop and implement a plan to resolve the failure or risk. The OCS must report annually to the Governor on any identified risk or failure to comply with established standards and policies. The OCS must review with the Governor on a quarterly basis any identified risks that are not mitigated. The report to the Governor is confidential and exempt from disclosure under the Public Records Act (PRA).

Independent Security Evaluation Audit. The Office of Financial Management must contract with an independent third party to audit the security and protection of digital assets. The purpose of the audit is to test and assess the state's overall security posture, including cybersecurity. Minimum audit requirements are prescribed. The independent audit team must provide monthly executive briefings to certain members of the Legislature on the progress of the audit being conducted. The final security audit report is due to the fiscal committees of the Legislature by August 31, 2022. Reports shared and submitted by the independent audit team are exempt from disclosure under the PRA.

Major Cybersecurity Incident Response.
Agencies must report any major cybersecurity incident to the OCS within 24 hours of discovering the incident. The OCS must then investigate the incident and facilitate any incident response measures necessary.

Report on Best Practices.
The OCS must collaborate with the OPDP and the Office of the Attorney General to research and examine best practices for data governance, data protection, sharing data relating to cybersecurity, and protection of state and local government IT systems and infrastructure. The research must include an examination of model terms for data sharing contracts and adherence to privacy principles. The OCS must report on its findings and specific recommendations to the Governor and Legislature by December 1, 2021.

Data Sharing Agreements.
Before sharing category 3 data or higher with a contractor, an agency must have a written data sharing agreement in place that conforms to statutory requirements on policies for data sharing.

A public agency that requests category 3 data or higher from another public agency must provide a written agreement between the agencies that conforms to the policies of the OCS.

Appropriation: None.

Fiscal Note: Requested on March 3, 2021.

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