S-2071.1

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**SENATE BILL 5474**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**State of Washington 67th Legislature 2021 Regular Session**

**By** Senator Mullet

AN ACT Relating to preparedness of state agencies to manage data backup and improve disaster recovery practices; creating new sections; and providing an expiration date.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

NEW SECTION. **Sec.**  The legislature recognizes that breaches in data security prevent state agencies from protecting confidential and sensitive information stored in information technology systems. In the absence of proper data backup and disaster recovery practices, state agency information technology systems are vulnerable to such breaches in security. The legislature finds that the office of the chief information officer has developed policies and standards for data backup and recovery practices that agencies are encouraged to emulate so as to protect confidential and sensitive information contained in each agency's information technology systems. On September 17, 2020, the state auditor's office released a performance audit regarding data backup and disaster recovery. Within these findings, the state auditor's office found that none of the four audited agencies fully and consistently met all state requirements for data backup, disaster recovery, and testing recovery plans. In addition to not meeting state requirements, the state auditor's office found agencies could further reduce disruptions to their services and operations by following the backup and disaster recovery guidance offered by leading practices. The legislature recognizes that action must be taken at each state agency to ensure data backup and disaster recovery practices are consistent with the office of the chief information officer's policies and standards for data backup and recovery practices to protect agencies from the harmful impacts of information technology systems disruptions.

NEW SECTION. **Sec.**  (1) By October 1, 2022, each executive state agency must perform a review of its internal data backup and disaster recovery practices, utilizing the policies and standards adopted by the office of the chief information officer under chapter 43.105 RCW, and must submit a report of its findings to the office of the chief information officer. The report must include:

(a) An evaluation of the agency's existing data backup and disaster recovery practices and how they compare to the policies and standards adopted by the office of the chief information officer under chapter 43.105 RCW; and

(b) If the agency's existing data backup and disaster recovery practices do not align with the policies and standards adopted by the office of the chief information officer under chapter 43.105 RCW, an analysis of the estimated costs and timelines required to achieve compliance with these standards.

(2) By December 1, 2022, the office of the chief information officer must submit to the legislature a report summarizing agency findings submitted pursuant to subsection (1) of this section, including agency compliance with data backup and disaster recovery standards and policies adopted under chapter 43.105 RCW, and aggregate agency estimated costs and timelines required to achieve compliance with these policies and standards.

NEW SECTION. **Sec.**  Sections 1 and 2 of this act expire June 30, 2023.

**--- END ---**