Multiple Agency Fiscal Note Summary

Bill Number: 5843 SB	**Title:** Election security breaches

Estimated Cash Receipts

NONE

Estimated Operating Expenditures

Agency Name	2023-25				2025-27				2027-29			
	FTEs	GF-State	NGF-Outlook	Total	FTEs	GF-State	NGF-Outlook	Total	FTEs	GF-State	NGF-Outlook	Total
Office of the Secretary of State	.0	81,000	81,000	81,000	.0	162,000	162,000	162,000	.0	162,000	162,000	162,000
Total $	**0.0**	**81,000**	**81,000**	**81,000**	**0.0**	**162,000**	**162,000**	**162,000**	**0.0**	**162,000**	**162,000**	**162,000**

Agency Name	2023-25			2025-27			2027-29		
	FTEs	GF-State	Total	FTEs	GF-State	Total	FTEs	GF-State	Total
Local Gov. Courts									
Loc School dist-SPI									
Local Gov. Other	Non-zero but indeterminate cost and/or savings. Please see discussion.								
Local Gov. Total									

Estimated Capital Budget Expenditures

Agency Name	2023-25			2025-27			2027-29		
	FTEs	Bonds	Total	FTEs	Bonds	Total	FTEs	Bonds	Total
Office of the Secretary of State	.0	0	0	.0	0	0	.0	0	0
Total $	**0.0**	**0**	**0**	**0.0**	**0**	**0**	**0.0**	**0**	**0**

Agency Name	2023-25			2025-27			2027-29		
	FTEs	GF-State	Total	FTEs	GF-State	Total	FTEs	GF-State	Total
Local Gov. Courts									
Loc School dist-SPI									
Local Gov. Other	Non-zero but indeterminate cost and/or savings. Please see discussion.								
Local Gov. Total									

Estimated Capital Budget Breakout

NONE

FNPID 68835

FNS029 Multi Agency rollup

Prepared by: Cheri Keller, OFM	Phone: (360) 584-2207	Date Published: Final 1/ 9/2024

Individual State Agency Fiscal Note

Bill Number: 5843 SB	Title: Election security breaches	Agency: 085-Office of the Secretary of State

Part I: Estimates

☐ **No Fiscal Impact**

Estimated Cash Receipts to:

NONE

Estimated Operating Expenditures from:

	FY 2024	FY 2025	2023-25	2025-27	2027-29
Account					
General Fund-State 001-1	0	81,000	81,000	162,000	162,000
Total $	0	81,000	81,000	162,000	162,000

Estimated Capital Budget Impact:

NONE

The cash receipts and expenditure estimates on this page represent the most likely fiscal impact. Factors impacting the precision of these estimates, and alternate ranges (if appropriate), are explained in Part II.

Check applicable boxes and follow corresponding instructions:

☒ If fiscal impact is greater than $50,000 per fiscal year in the current biennium or in subsequent biennia, complete entire fiscal note form Parts I-V.

☐ If fiscal impact is less than $50,000 per fiscal year in the current biennium or in subsequent biennia, complete this page only (Part I).

☐ Capital budget impact, complete Part IV.

☐ Requires new rule making, complete Part V.

Legislative Contact:	Greg Vogel	Phone: 360-786-7413	Date: 01/02/2024
Agency Preparation:	Mike Woods	Phone: (360) 704-5215	Date: 01/09/2024
Agency Approval:	Mike Woods	Phone: (360) 704-5215	Date: 01/09/2024
OFM Review:	Cheri Keller	Phone: (360) 584-2207	Date: 01/09/2024

Part II: Narrative Explanation

II. A - Brief Description Of What The Measure Does That Has Fiscal Impact

Significant provisions of the bill and any related workload or policy assumptions that have revenue or expenditure impact on the responding agency by section number.

Section 1(2) of this bill requires each county to install and maintain an intrusion detection system that passively monitors its network for malicious traffic 24 hours a day, seven days a week, and 365 days a year by a qualified and trained security team with access to cyber incident response personnel who can assist the county in the event of a malicious attack. The system must support the unique security requirements of state, local, tribal, and territorial governments and possess the ability to receive cyber intelligent threat updates to stay ahead of evolving attack patterns.

II. B - Cash receipts Impact

Cash receipts impact of the legislation on the responding agency with the cash receipts provisions identified by section number and when appropriate, the detail of the revenue sources. Description of the factual basis of the assumptions and the method by which the cash receipts impact is derived. Explanation of how workload assumptions translate into estimates. Distinguished between one time and ongoing functions.

II. C - Expenditures

Agency expenditures necessary to implement this legislation (or savings resulting from this legislation), with the provisions of the legislation that result in the expenditures (or savings) identified by section number. Description of the factual basis of the assumptions and the method by which the expenditure impact is derived. Explanation of how workload assumptions translate into cost estimates. Distinguished between one time and ongoing functions.

The Office of the Secretary of State (OSOS) currently pays the fee for such an intrusion detection system for 31 counties through Section 120(7) in ESSB 5187. In FY 2024, OSOS renewed the cost of these systems for $459,210.00. Another five counties also have installed and maintain these same systems, the funding for which they obtain directly through the Department of Homeland Security. Under SB 5843, OSOS assumes an additional $81,000 (an average of $27,000 per county) through the abovementioned proviso for three more county systems will be required.

Part III: Expenditure Detail

III. A - Operating Budget Expenditures

Account	Account Title	Type	FY 2024	FY 2025	2023-25	2025-27	2027-29
001-1	General Fund	State	0	81,000	81,000	162,000	162,000
		Total $	0	81,000	81,000	162,000	162,000

III. B - Expenditures by Object Or Purpose

	FY 2024	FY 2025	2023-25	2025-27	2027-29
FTE Staff Years					
A-Salaries and Wages					
B-Employee Benefits					
C-Professional Service Contracts					
E-Goods and Other Services					
G-Travel					
J-Capital Outlays					
M-Inter Agency/Fund Transfers					
N-Grants, Benefits & Client Services		81,000	81,000	162,000	162,000
P-Debt Service					
S-Interagency Reimbursements					
T-Intra-Agency Reimbursements					
9-					
Total $	0	81,000	81,000	162,000	162,000

III. C - Operating FTE Detail: *FTEs listed by classification and corresponding annual compensation. Totals agree with total FTEs in Part I and Part IIIA.*

NONE

III. D - Expenditures By Program (optional)

NONE

Part IV: Capital Budget Impact

IV. A - Capital Budget Expenditures

NONE

IV. B - Expenditures by Object Or Purpose

NONE

IV. C - Capital Budget Breakout

Acquisition and construction costs not reflected elsewhere on the fiscal note and description of potential financing methods.

NONE

IV. D - Capital FTE Detail: *FTEs listed by classification and corresponding annual compensation. Totals agree with total FTEs in Part IVB.*

NONE

Part V: New Rule Making Required

Provisions of the bill that require the agency to adopt new administrative rules or repeal/revise existing rules.

LOCAL GOVERNMENT FISCAL NOTE

Department of Commerce

Bill Number: 5843 SB	Title: Election security breaches

Part I: Jurisdiction-Location, type or status of political subdivision defines range of fiscal impacts.

Legislation Impacts:

☐ Cities:

☒ Counties: County auditors could experience indeterminate costs associated with new intrusion detection monitoring systems

☐ Special Districts:

☐ Specific jurisdictions only:

☐ Variance occurs due to:

Part II: Estimates

☐ No fiscal impacts.

☐ Expenditures represent one-time costs:

☐ Legislation provides local option:

☒ Key variables cannot be estimated with certainty at this time: The number of counties that may already have monitoring systems that would comply with the legislation's requirements; the number of cyber incident response personnel that would need to be hired; cost to update training materials, and the time required to train new staff

Estimated revenue impacts to:

None

Estimated expenditure impacts to:

Non-zero but indeterminate cost and/or savings. Please see discussion.

Part III: Preparation and Approval

Fiscal Note Analyst: Kate Fernald	Phone: 564-200-3519	Date: 01/09/2024
Leg. Committee Contact: Greg Vogel	Phone: 360-786-7413	Date: 01/02/2024
Agency Approval: Allan Johnson	Phone: 360-725-5033	Date: 01/09/2024
OFM Review: Cheri Keller	Phone: (360) 584-2207	Date: 01/09/2024

Part IV: Analysis

A. SUMMARY OF BILL

Description of the bill with an emphasis on how it impacts local government.

Sec. 1 would amend RCW 29A.12.180.

Sec. 1 (2) would require every county to install and maintain an intrusion detection system that passively monitors its network for malicious traffic by a qualified and trained security team with access to cyber incident response personnel who can assist the county in the event of a malicious attack. The system would be required to support the unique security requirements of state, local, tribal, and territorial governments and possess the ability to receive cyber intelligence threat updates to stay ahead of evolving attack patterns.

Sec. 1 (3) would require the county auditor or county information technology director of any county, participating in the shared voter registration system, or operating a voting system or component of a voting system certified by the Secretary of State, must disclose to the Secretary of State and attorney general any malicious activity or breach of the security of any of its information technology systems immediately following discovery if:

(a) malicious activity was detected by an information technology (IT) intrusion detection system, malicious domain blocking and reporting system, or endpoint security software;

(b) a breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of election systems, IT systems used to manage the administration of elections, or peripheral IT systems that support the county auditor's office in day-to-day activities;

(c) the breach has, or is reasonably likely to have, compromised the security, confidentiality, or integrity of an election within the state; or

(d) personal information of residents in any state was, or is reasonably believed to have been, acquired by an unauthorized person as a result of the breach and the personal information was not secured.

Sec. 1 (4) (a) For the purpose of this section, “malicious activity” would be defined as an external or internal threat that is designed to damage, disrupt, or compromise an information technology network, as well as the hardware and application that reside on the network, thereby impacting performance, data integrity, and the confidentiality of data on the network. Threats include: viruses, ransomware, Trojan horses, worms, malware, data loss, or the disabling or removing of information technology security systems.

Sec. 1 (4) (b) For the purpose of this section, “security breach” would be defined as a breach of the election system, information technology systems used to administer and support the election process, or associated data where the system or associated data has been penetrated, accessed, or manipulated by an unauthorized person. The definition of breach includes all unauthorized access to systems by external or internal personnel or organizations, including personnel employed by a county or the state providing access to systems that have the potential to lead to a breach.

Sec. 2 amends RCW 29A.12.200.

Sec. 2 (4) (a) For purposes of the Secretary of State's annual report on election security breaches, "domestic entity" would be defined as an entity organized or formed under the laws of the United States, a person domiciled in the United States, or a citizen of the United States.

Sec. 3 amends RCW 29A.40.100 and would clarify that observers may not touch any ballots, ballot materials, or election systems. Unauthorized physical contact, or access to ballots or election systems would be specified as a crime subject to punishment under chapter 29A.84 RCW.

Sec. 4 amends RCW 29A.40.160.

Sec. 4 (8) would directly state that no person may interfere with the operation of a voting center. It lists what is prohibited and explains that unauthorized access includes elected officials and county staff accessing systems in any manner not required by their job function.

Sec. 5 would amend RCW 29A.60.200.

Sec. 5 (3) would establish an election certification plan when a county canvassing board refuses to certify an election without cause. If a county canvassing board refuses to certify the results of an election without cause, the Secretary of State would be allowed to examine the records, ballots, and results of the election and certify the results of the election. The Secretary of State's certification would be required to be completed within two business days after the certification deadline for the election after the refusal of the county canvassing board to certify the results of the election.

Sec. 6 amends RCW 29A.84.550 and would add election office, ballot counting area, ballot storage area, or election system including materials and systems meant for enabling a voter to prepare the voter's ballot to the list of places at which a class C felony will be punishable if any person willfully defaces, removes or destroys any of the supplies or materials that the person knows are intended both for use in a voting center and for enabling a voter to prepare the voter's ballot.

Sec. 7 would establish a new section to be added to chapter 29A.84 RCW to clarify who would be guilty of a class C felony punishable under RCW 9A.20.021.

Sec. 8 would amend RCW 29A.84.560 to clarify who would be guilty of a class C felony if they tampered with, damaged or attempted to damage any voting machine or device to be used in a primary or general election.

Sec. 9 amends RCW 29A.84.720 to expand the actions that would result in a class C felony. Every person charged with the performance of any duty under state or local election laws, who provides unauthorized access to a person or entity to physical locations or electronic or physical access to election software or hardware used in any element of conduct of an election is guilty of a class C felony and must forfeit their office.

Sec. 10 amends RCW 29A.84.050 to clarify that any person who knowingly destroys, alters, defaces, conceals, or discards a voted ballot would be guilty of a gross misdemeanor. As well, any person who intentionally fails to return another person's voted ballot to the proper state or county elections office by the applicable deadline would be guilty of a gross misdemeanor.

B. SUMMARY OF EXPENDITURE IMPACTS

Expenditure impacts of the legislation on local governments with the expenditure provisions identified by section number and when appropriate, the detail of expenditures. Delineated between city, county and special district impacts.

The proposed legislation's expenditure impact on local governments is indeterminate until additional information is available to determine workload impacts.

Auditors could experience indeterminate impacts associated with purchasing a security system; hiring a qualified and trained security team; and hiring cyber incident response personnel who could assist the county in the event of a malicious attack. County auditors could also incur expenditure increases for updating their training materials and training their current staff on violations and penalties related to election interference.

Without additional information, however, expenditure impacts cannot be calculated. Therefore, the expenditure impact of the proposed legislation is indeterminate until additional information is available.

C. SUMMARY OF REVENUE IMPACTS

Revenue impacts of the legislation on local governments, with the revenue provisions identified by section number, and when appropriate, the detail of revenue sources. Delineated between city, county and special district impacts.

The proposed legislation would not impact local governments' revenue.

SOURCES:
Washington State Association of County Auditors