

Multiple Agency Fiscal Note Summary

Bill Number: 5619 SB	Title: Cybersecurity governance
-----------------------------	--

Estimated Cash Receipts

Agency Name	2023-25			2025-27			2027-29		
	GF-State	NGF-Outlook	Total	GF-State	NGF-Outlook	Total	GF-State	NGF-Outlook	Total
Consolidated Technology Services	0	0	134,000	0	0	134,000	0	0	134,000
Total \$	0	0	134,000	0	0	134,000	0	0	134,000

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
Consolidated Technology Services	.5	0	0	134,000	.5	0	0	134,000	.5	0	0	134,000
Military Department	1.0	268,372	268,372	268,372	1.0	263,372	263,372	263,372	1.0	263,372	263,372	263,372
Total \$	1.5	268,372	268,372	402,372	1.5	263,372	263,372	397,372	1.5	263,372	263,372	397,372

Estimated Capital Budget Expenditures

Agency Name	2023-25			2025-27			2027-29		
	FTEs	Bonds	Total	FTEs	Bonds	Total	FTEs	Bonds	Total
Consolidated Technology Services	.0	0	0	.0	0	0	.0	0	0
Military Department	.0	0	0	.0	0	0	.0	0	0
Total \$	0.0	0	0	0.0	0	0	0.0	0	0

Estimated Capital Budget Breakout

NONE

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

Individual State Agency Fiscal Note

Bill Number: 5619 SB	Title: Cybersecurity governance	Agency: 163-Consolidated Technology Services
-----------------------------	--	---

Part I: Estimates

No Fiscal Impact

Estimated Cash Receipts to:

ACCOUNT	FY 2024	FY 2025	2023-25	2025-27	2027-29
Consolidated Technology Services	67,000	67,000	134,000	134,000	134,000
Revolving Account-State 458-1					
Total \$	67,000	67,000	134,000	134,000	134,000

Estimated Operating Expenditures from:

	FY 2024	FY 2025	2023-25	2025-27	2027-29
FTE Staff Years	0.5	0.5	0.5	0.5	0.5
Account					
Consolidated Technology Services	67,000	67,000	134,000	134,000	134,000
Revolving Account-State 458-1					
Total \$	67,000	67,000	134,000	134,000	134,000

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: Angela Kleis	Phone: 360-786-7469	Date: 01/28/2023
Agency Preparation: Nenita Ching	Phone: 360-407-8878	Date: 02/02/2023
Agency Approval: Tim Gallivan	Phone: (360) 407-8215	Date: 02/02/2023
OFM Review: Cheri Keller	Phone: (360) 584-2207	Date: 02/03/2023

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.

This bill would codify a subcommittee of the Technology Services Board (TSB) dedicated to cybersecurity. It would also require a state of cybersecurity report be completed each year jointly by the Military Department and WaTech.

Section 1 requires the cybersecurity advisory committee created out of the emergency management council to meet with the TSB cybersecurity subcommittee once a year.

Section 2 creates a new cybersecurity subcommittee of the TSB by adding a new section to 43.105.

Subsection 1 specifies membership of the TSB security subcommittee, and allows the chair to make additional appointments as necessary to ensure relevant sectors are represented.

Subsection 2 specifies the duties of the TSB security subcommittee, to include the following:

- a) Review emergent cyberattacks and threats to critical infrastructure sectors in order to identify existing gaps in state agency cybersecurity policies;
- b) Assess emerging risks to state agency information technology;
- c) Recommend a reporting and information sharing system to notify state agencies of new risks, risk treatment opportunities, and projected shortfalls in response and recovery;
- d) Recommend tabletop cybersecurity exercises, including data breach simulation exercises;
- e) Assist the office of cybersecurity created in RCW 43.105.450 in developing cybersecurity best practice recommendations for state agencies;
- f) Review the proposed policies and standards developed by the office of cybersecurity and recommend their approval to the full board;
- g) Review information relating to cybersecurity incidents and ransomware incidents to determine commonalities and develop best practice recommendations for public agencies; and
- h) Assist the agency and the military department in creating the state of cybersecurity report required in subsection (6) of this section.

Subsection 3 directs WaTech, as part of its staffing of the security subcommittee, to work with NIST and other federal agencies, private sector business and cybersecurity experts to bring their experience and guidance to the board for consideration.

Subsection 4 allows for a portion of the agenda to be conducted in executive session closed to the public. No more than half the agenda time may be dedicated to executive session.

Subsection 5 requires the subcommittee to meet at least quarterly, and at least annually meet with the cybersecurity advisory committee of the emergency management council created in Section 2.

Subsection 6 requires an annual report to the governor and appropriate committees of the legislature on December 1, 2023, and each December 1 thereafter, to be produced on the state of cybersecurity. The report is the joint responsibility of the military department and of WaTech. The TSB security subcommittee has the authority to identify as confidential and not subject to disclosure portions of the report deemed necessary to protect the security of public and private cyber systems.

Subsection 7 directs WaTech and the cybersecurity subcommittee to collaborate with the military department and the cybersecurity advisory committee of the emergency management council created above.

Subsection 8 notes that the reports produced and information are confidential and not subject to disclosure under RCW

42.56.

Section 3 adds the exemption to 42.56 for the reports required in this subsection.

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.

The Office of the Chief Information Officer (OCIO) is funded by an appropriation from the Consolidated Technology Services Revolving Account (458-1.) Revenues for the OCIO are collected from state agencies who receive allocations through the central services model. It is assumed that the allocations in the central services model will be adjusted by the Legislature to ensure WaTech revenues are sufficient to support the required expenditures.

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.

Section 2, subsection 2 specifies the duties of the TSB security subcommittee, to include the following:

- a) Review emergent cyberattacks and threats to critical infrastructure sectors in order to identify existing gaps in state agency cybersecurity policies;
- b) Assess emerging risks to state agency information technology;
- c) Recommend a reporting and information sharing system to notify state agencies of new risks, risk treatment opportunities, and projected shortfalls in response and recovery;
- d) Recommend tabletop cybersecurity exercises, including data breach simulation exercises;
- e) Assist the office of cybersecurity created in RCW 43.105.450 in developing cybersecurity best practice recommendations for state agencies;
- f) Review the proposed policies and standards developed by the office of cybersecurity and recommend their approval to the full board;
- g) Review information relating to cybersecurity incidents and ransomware incidents to determine commonalities and develop best practice recommendations for public agencies; and
- h) Assist the agency and the military department in creating the state of cybersecurity report required in subsection (6) of this section.

Section 2, subsection 3 directs WaTech, as part of its staffing of the security subcommittee, to work with NIST and other federal agencies, private sector business and cybersecurity experts to bring their experience and guidance to the board for consideration.

Section 2, subsection 5 requires the subcommittee to meet at least quarterly, and at least annually meet with the cybersecurity advisory committee of the emergency management council created in Section 2.

Section 2, subsection 6 requires an annual report to the governor and appropriate committees of the legislature on December 1, 2023, and each December 1 thereafter, to be produced on the state of cybersecurity. The report is the joint responsibility of the military department and of WaTech.

A Management Analyst 3 (0.5 FTE) is required to adequately staff the TSB security subcommittee to meet the requirements stated above. This would include coordinating work with the Military Department, federal agencies, and private sector businesses as required in the bill. This FTE would also be responsible for coordinating with our Records Management Unit on the preparation of meeting materials and the annual report, to determine what portions, if any, should be made confidential and not subject to disclosure.

The annual costs are estimated to be \$67,000 (\$59,000 for salary and benefits, \$1,000 for goods and services, training, and

travel, and \$7,000 for overhead and shared services).

Part III: Expenditure Detail

III. A - Operating Budget Expenditures

Account	Account Title	Type	FY 2024	FY 2025	2023-25	2025-27	2027-29
458-1	Consolidated Technology Services Revolving Account	State	67,000	67,000	134,000	134,000	134,000
Total \$			67,000	67,000	134,000	134,000	134,000

III. B - Expenditures by Object Or Purpose

	FY 2024	FY 2025	2023-25	2025-27	2027-29
FTE Staff Years	0.5	0.5	0.5	0.5	0.5
A-Salaries and Wages	37,000	37,000	74,000	74,000	74,000
B-Employee Benefits	22,000	22,000	44,000	44,000	44,000
C-Professional Service Contracts					
E-Goods and Other Services	1,000	1,000	2,000	2,000	2,000
G-Travel					
J-Capital Outlays					
M-Inter Agency/Fund Transfers					
N-Grants, Benefits & Client Services					
P-Debt Service					
S-Interagency Reimbursements					
T-Intra-Agency Reimbursements	7,000	7,000	14,000	14,000	14,000
9-					
Total \$	67,000	67,000	134,000	134,000	134,000

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

Job Classification	Salary	FY 2024	FY 2025	2023-25	2025-27	2027-29
Management Analyst 3	74,000	0.5	0.5	0.5	0.5	0.5
Total FTEs		0.5	0.5	0.5	0.5	0.5

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.

Individual State Agency Fiscal Note

Bill Number: 5619 SB	Title: Cybersecurity governance	Agency: 245-Military Department
-----------------------------	--	--

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
FTE Staff Years	1.0	1.0	1.0	1.0	1.0
Account					
General Fund-State 001-1	136,686	131,686	268,372	263,372	263,372
Total \$	136,686	131,686	268,372	263,372	263,372

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: Angela Kleis	Phone: 360-786-7469	Date: 01/28/2023
Agency Preparation: Serina Roberts	Phone: 2535127388	Date: 02/02/2023
Agency Approval: Timothy Rajcevich	Phone: 2535127596	Date: 02/02/2023
OFM Review: Cheri Keller	Phone: (360) 584-2207	Date: 02/02/2023

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 1.4.a – development of recommendations to strengthen cyber resilience for the public sector, private industry, and all critical infrastructure sectors (energy, transportation, water, communications, chemical, elections, education, healthcare, etc)
- Section 1.4.b – coordination of the cybersecurity advisory committee to include public sector and industry partners, and all critical infrastructure sectors.
- Section 1.4.b.i – assessing infrastructure not covered by federal law
- Section 1.4.b.ii – using federal guidance to identify categories of critical infrastructure as critical cyber infrastructure to prevent and protect against cyber damage
- Section 1.4.b.iii – recommending cyber exercises with critical infrastructure sectors
- Section 1.4.b.iv – examine inconsistencies between state and federal law
- Section 1.4.c – coordination with WaTech and the technology services board
- Section 1.4.d – conducting secure meetings and redact sensitive information in compliance with the protected critical infrastructure information program
- Section 1.4.e – conduct quarterly meetings and meet with WaTech

All of the above require dedicated staff time to manage and conduct. Most of the above require expert-level knowledge of technology issues, systems interdependencies, legal statutes, and homeland security practices.

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.

- 1 full-time position (EMPS-3)
- Travel to discuss sensitive issues, threats, and vulnerabilities with stakeholders
- Coordination and management of Cybersecurity Advisory Committee

The expenditures would fund staff time and effort to meet the intent of the bill prescribed in the following sections:

- Section 1.4.a – development of recommendations to strengthen cyber resilience for the public sector, private industry, and all critical infrastructure sectors (energy, transportation, water, communications, chemical, elections, education, healthcare, etc)
- Section 1.4.b – coordination of the cybersecurity advisory committee to include public sector and industry partners, and all critical infrastructure sectors.
- Section 1.4.b.i – assessing infrastructure not covered by federal law
- Section 1.4.b.ii – using federal guidance to identify categories of critical infrastructure as critical cyber infrastructure to prevent and protect against cyber damage
- Section 1.4.b.iii – recommending cyber exercises with critical infrastructure sectors
- Section 1.4.b.iv – examine inconsistencies between state and federal law
- Section 1.4.c – coordination with WaTech and the technology services board
- Section 1.4.d – conducting secure meetings and redact sensitive information in compliance with the protected critical infrastructure information program
- Section 1.4.e – conduct quarterly meetings and meet with WaTech

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	136,686	131,686	268,372	263,372	263,372
Total \$			136,686	131,686	268,372	263,372	263,372

III. B - Expenditures by Object Or Purpose

	FY 2024	FY 2025	2023-25	2025-27	2027-29
FTE Staff Years	1.0	1.0	1.0	1.0	1.0
A-Salaries and Wages	82,896	82,896	165,792	165,792	165,792
B-Employee Benefits	39,790	39,790	79,580	79,580	79,580
C-Professional Service Contracts					
E-Goods and Other Services	5,000	5,000	10,000	10,000	10,000
G-Travel	4,000	4,000	8,000	8,000	8,000
J-Capital Outlays	5,000		5,000		
M-Inter Agency/Fund Transfers					
N-Grants, Benefits & Client Services					
P-Debt Service					
S-Interagency Reimbursements					
T-Intra-Agency Reimbursements					
9-					
Total \$	136,686	131,686	268,372	263,372	263,372

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

Job Classification	Salary	FY 2024	FY 2025	2023-25	2025-27	2027-29
Emergency Management Program Specialist 3	82,896	1.0	1.0	1.0	1.0	1.0
Total FTEs		1.0	1.0	1.0	1.0	1.0

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.