SB 18-086

Legislative Council Staff

Nonpartisan Services for Colorado's Legislature

FISCAL NOTE

Drafting Number:	LLS 18-0326	**Date:**	February 5, 2018
Prime Sponsors:	Sen. Lambert; Williams A. Rep. Ginal; Rankin	**Bill Status:**	Senate Business
		Fiscal Analyst:	Kerry White | 303-866-3469 Kerry.White@state.co.us

Bill Topic: CYBER CODING CRYPTOLOGY FOR STATE RECORDS

Summary of Fiscal Impact:

- ☐ State Revenue
- ☒ State Expenditure
- ☐ State Transfer
- ☐ TABOR Refund
- ☐ Local Government
- ☐ Statutory Public Entity

This bill requires the state's Chief Information Security Officer to annually identify, assess, and mitigate cyber threats to the state and encourages the state to adopt and apply distributed ledger technologies in its data systems where feasible. The bill increases state expenditures beginning in FY 2018-19.

Appropriation Summary: For FY 2018-19, the bill requires an appropriation of $250,000 to the Office of Information Technology.

Fiscal Note Status: The fiscal note reflects the introduced bill.

Table 1
State Fiscal Impacts Under SB 18-086

		FY 2018-19	FY 2019-20
Revenue		-	-
Expenditures	General Fund	$250,000	not estimated
Transfers		-	-

Summary of Legislation

This bill requires the state's Chief Information Security Officer (CISO) to annually identify, assess, and mitigate cyber threats to the state. The CISO is required to annually collect information through public agency enterprise cybersecurity plans in order to assess the nature of threats to data systems and the potential risks and liabilities. This requirement applies to all units of state government except the General Assembly and institutions of higher education, which are permitted to participate.

State data systems. In coordination with the Colorado Cybersecurity Council, the Office of Information Technology (OIT) and the Government Data Advisory Board, the CISO is encouraged to:

- develop and maintain a series of metrics and to assess the data systems of each public agency for the benefits and costs of adopting and applying distributed ledger technologies;
- consider developing public-private partnerships and contracts to allow capitalization of encryption technologies; and
- ensure that platforms incorporate the nonrepudiation (inability to deny the authenticity of signatures) of participating entities in virtual transactions.

Department of State. The Department of State is required to consider research, development, and implementation for appropriate encryption and data integrity, including distributed ledger technologies, after it accepts business licensing records and upgrades its business suite. When distributing data to other public agencies, the department is required to consider using distributed ledger technologies.

University of Colorado at Colorado Springs. The university is authorized to include distributed ledger technologies within its curricula and research and development activities.

Department of Regulatory Agencies. The Department of Regulatory Agencies (DORA) is directed to, in conjunction with OIT, consider secure encryption methods, especially distributed ledger technologies, for its data systems.

Office of Information Technology. In the administration of any new major information technology project, the OIT, working with the affected state agency, must evaluate the potential use of blockchain and distributed ledger technologies as part of the project. OIT must also conduct an assessment and present recommendations for a blockchain implementation project to the Joint Technology Committee of the General Assembly.

Background

A distributed ledger is a database that is shared and synchronized across multiple sites. It allows transactions to have public "witnesses," and may improve security because all of the distributed copies need to be attacked simultaneously for an attack to be successful. Blockchains are an underlying technology that can be used in a distributed ledger. A blockchain is a continuously growing list of records, called blocks, which are linked and secured using cryptography (encryption). Each block typically contains a timestamp and transaction data.

SB 18-086

The Department of Personnel and Administration has a decision item request of $375,000 pending before the Joint Budget Committee to add a cybersecurity liability insurance policy to its risk management program. If approved, the policy would help a state organization to offset recovery costs and indemnify the state for losses following a cyber-related security breach or similar event.

State Expenditures

The bill increases state General Fund expenditures in the Office of Information Technology by $250,000. Funds will be used to hire a contractor to conduct the required assessment. The fiscal note assumes that a request for proposals may occur in the current FY 2017-18, but that costs for the study will begin in FY 2018-19.

Future costs. Depending on the outcome of the study and efforts by OIT, state agencies, including the Department of State and DORA, could incur future implementation-related workload and costs related to distributed ledger technologies. The fiscal note assumes that implementation requirements will be included in separate legislation or through the annual budget process once the assessment is complete and recommendations are made to the Joint Technology Committee.

University of Colorado at Colorado Springs. The bill grants permission to the university to include distributed ledger technologies in its curricula and research and development activities. This analysis assumes that any increased workload and costs will be accommodated through existing budgets.

Effective Date

The bill takes effect upon signature of the Governor, or upon becoming law without his signature.

State Appropriations

For FY 2018-19, the bill requires an appropriation of $250,000 General Fund to the Office of Information Technology.

State and Local Government Contacts

All State Agencies