SB 18-086

Legislative Council Staff
Nonpartisan Services for Colorado's Legislature

REVISED FISCAL NOTE

(replaces fiscal note dated February 5, 2018)

Drafting Number:	LLS 18-0326	**Date:**	March 27, 2018
Prime Sponsors:	Sen. Lambert; Williams A. Rep. Ginal; Rankin	**Bill Status:**	Senate Appropriations
		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. State expenditures increase beginning in FY 2018-19.

Appropriation Summary: For FY 2018-19, the bill requires an appropriation of $9.8 million to multiple agencies.

Fiscal Note Status: The fiscal note reflects the introduced bill, as amended by the Senate Business, Labor, and Technology Committee.

Table 1
State Fiscal Impacts Under SB 18-086

		FY 2018-19	FY 2019-20
Revenue		-	-
Expenditures	General Fund	$9,800,000	$9,800,000
	FTE	1.0 FTE	1.0 FTE
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.

Local requirements. A county or municipal government may not impose a tax or fee on the use of distributed ledger technologies by any private person or entity or require any private person or entity to obtain a certificate, license, or permit from any public agency to use distributed ledger technologies.

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.

State Expenditures

The bill increases state General Fund expenditures by $9.8 million and 1.0 FTE per year, beginning in FY 2018-19.

Office of Information Technology. A total of $5 million and 1.0 FTE are required to fund OIT's efforts to mitigate cyberthreats and improve the state's security posture, as authorized by the bill. Funding will be used to implement and expand standardized security technology; privileged access management; cloud architecture and security governance; workforce technical security training; availability of skilled technical resources to implement security projects and to monitor security threats; and continuous reassessment of the existing security program, including ongoing enterprise risk management. Funds may also be required to conduct an assessment of systems, which is anticipated to cost $250,000. The fiscal note assumes that a request for proposals may occur in the current FY 2017-18, but if implemented, costs for a study would begin in FY 2018-19.

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, as well as to provide training to state and local government agencies. Costs of $2.8 million are anticipated in FY 2018-19 for these purposes.

Other institutions of higher education. Costs will increase by $2.0 million for the Colorado State University ($1.2 million for research and engagement), Colorado Mesa University ($300,000 for professional education), Pikes Peak Community College ($300,000 for professional education), and Western Colorado State University ($200,000 to expand offerings in information assurance, network security, hacking and malware).

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.

Local Government

The bill prohibits a county or municipal government from raising revenue through taxes, fees, certificates, and licenses related to distributed ledger technologies. As of this writing, it is assumed that revenue is not currently raised for these purposes.

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 $5,000,000 General Fund and an allocation of 1.0 FTE to the Office of Information Technology.

In addition, $4,800,000 should be appropriated to the Department of Higher Education for allocation as follows:

- $2,800,000 to the University of Colorado at Colorado Springs;
- $1,200,000 to the Colorado State University;
- $300,000 to the Colorado Mesa University;
- $300,000 to the Pikes Peak Community College; and
- $200,000 to Western Colorado State University.

State and Local Government Contacts

Counties	Information Technology
Municipalities	Revenue