LB651
2023

LEGISLATURE OF NEBRASKA

ONE HUNDRED EIGHTH LEGISLATURE

FIRST SESSION

LEGISLATIVE BILL 651

Introduced by McDonnell, 5.

Read first time January 18, 2023

Committee: Appropriations

A BILL FOR AN ACT relating to appropriations for cybersecurity; to state findings; to provide duties for the office of Chief Information Officer relating to cybersecurity; to provide funding for enhancing political subdivisions' cybersecurity; and to declare an emergency.

Be it enacted by the people of the State of Nebraska,

LB651
2023

Section 1. (1) For purposes of this section:

(a) Office means the office of the Chief Information Officer; and

(b) Political subdivision means villages, cities, counties, school districts, educational service units, and natural resource districts.

(2) The Legislature hereby finds and declares that:

(a) Cybersecurity is a growing problem for the State of Nebraska and its political subdivisions;

(b) The office of Chief Information Officer is constrained in its cybersecurity efforts due to its lack of General Fund appropriations from the Nebraska Legislature. Therefore, the office relies entirely on charging state agencies for services, resulting in increased costs for state agencies;

(c) The office, the state, and political subdivisions face sophisticated attacks from cyber adversaries and must act to defend networks, systems, and data from such attacks;

(d) The office must have access to the most advanced tools, software, and services, to combat cyber threats against the state and its political subdivisions;

(e) The state and its executive agencies contract with thousands of vendors, each of which could pose a cybersecurity threat to the state and the services that Nebraska residents rely upon. As such, the Chief Information Officer must have insight into the cybersecurity vulnerabilities of entities doing business with the state; and

(f) In addressing these issues, the office will need to establish strategic partnerships and contracts with companies that are in compliance with state and federal cybersecurity standards.

(3) It is the intent of the Legislature to appropriate twenty million dollars of General Funds annually beginning in FY2023-24 to Agency 65, Department of Administrative Services, Program 172, Information Management Services Division, for the purposes of cybersecurity activities described in this section.

LB651
2023

(4)(a) The office shall work to:

(i) Support cybersecurity preparedness activities;

(ii) Procure tools, hardware, software, or services, that enhance or expand the cybersecurity defense and response capabilities of the state;

(iii) Strengthen and expand cyber risk management activities for the state;

(iv) Expand vulnerability monitoring, identification, and management;

(v) Increase and maintain cyber incident response capabilities;

(vi) Promote cybersecurity training and awareness within the state; and

(vii) Support cybersecurity workforce development within the state;

(b) It is the intent of the Legislature that of the appropriation described in subsection (3) of this section, three million dollars of such appropriation be used annually for purposes of this subsection, including up to one million dollars in total expenditures for permanent and temporary salaries and per diems.

(5)(a) The office shall work to secure and remediate the cybersecurity vulnerabilities within the vendor ecosystems of vendors contracted with the state, executive agencies, and political subdivisions by contracting with a software provider that will:

(i) Provide the office access to publicly observable cybersecurity vulnerabilities of state and executive agencies vendors. Such information shall be updated daily to ensure action may be taken if deemed necessary by the Chief Information Officer;

(ii) Notify state executive agencies' vendors of specific vulnerabilities, as defined by the Chief Information Officer, and track the remediation efforts of vendors deemed critical by the Chief Information Officer; and

(iii) Provide political subdivisions the ability to monitor publicly observable cybersecurity vulnerabilities of themselves and their vendor

LB651
2023

ecosystems and training classes on managing their cybersecurity vendor ecosystems.

(b) It is the intent of the Legislature that of the appropriation described in subsection (3) of this section, eight million dollars of such appropriation be used annually for purposes of this subsection.

(6)(a) A program is created to provide political subdivisions the ability to upgrade critical information technology infrastructure. The program shall be administered by the office.

(b) A political subdivision may apply for funding under this subsection by submitting an application to the office in a form and manner prescribed by the office.

(c) The office shall develop eligibility criteria under this subsection. At a minimum, the eligibility criteria shall require a political subdivision to document how the money will be used to fulfill the purposes and requirements set forth in subdivision (6)(d) of this section.

(d) A political subdivision awarded money under this subsection shall use such money to upgrade critical information technology infrastructure of the political subdivision, improve training on cybersecurity, and work toward compliance with nationally recognized cybersecurity frameworks and other cybersecurity objectives outlined by the Chief Information Officer.

(e) The office may adopt and promulgate rules and regulations to carry out this subsection, including, but not limited to, defining what qualifies as critical information technology infrastructure, setting parameters for cybersecurity training, selecting cybersecurity frameworks, and methods and metrics for determining political subdivisions' progress toward compliance with such frameworks.

(f) Each fiscal year, money remaining in the program that is not provided to political subdivisions due to a lack of qualifying applicants or projects may be used by the office to upgrade the state's critical

information technology infrastructure.

(g) It is the intent of the Legislature that of the appropriation described in subsection (3) of this section, four million five hundred thousand dollars of such appropriation be used annually for purposes of this subsection, including up to five hundred thousand dollars in total expenditures for permanent and temporary salaries and per diems.

(7)(a) The office shall purchase software and services, including, but not limited to, identity access management, cybersecurity incident response capabilities, cybersecurity training, and other activities that promote cybersecurity, and make such software and services available to political subdivisions at no cost. The Chief Information Officer may include services to be used by the state and state agencies as long as the contracted software or services are offered to political subdivisions at no charge.

(b) It is the intent of the Legislature that of the appropriation described in subsection (3) of this section, four million five hundred thousand dollars of such appropriation be used annually for purposes of this subsection, including up to two hundred fifty thousand dollars in total expenditures for permanent and temporary salaries and per diems.

(8) In negotiating contracts for this section, the office shall, if practicable, use vendors associated with existing procurement contracts with the office.

(9) Any person that the office enters into a contract with to purchase software or services pursuant to this section shall:

(a) Be headquartered in the United States;

(b) Be in good standing in this state; and

(c) Have demonstrated the ability to achieve the "Ready" stage in the Federal Risk and Authorization Management Program (FedRAMP) certification process, as determined by the office.

Sec. 2. Since an emergency exists, this act takes effect when passed and approved according to law.