LB1302
2024

LEGISLATURE OF NEBRASKA

ONE HUNDRED EIGHTH LEGISLATURE

SECOND SESSION

LEGISLATIVE BILL 1302

Introduced by Lippincott, 34; Aguilar, 35; DeKay, 40; Holdcroft, 36.

Read first time January 17, 2024

Committee: Government, Military and Veterans Affairs

A BILL FOR AN ACT relating to cybersecurity; to adopt the Cybersecurity Preparedness Act; and to declare an emergency.

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

LB1302
2024

Section 1. Sections 1 to 12 of this act shall be known and may be cited as the Cybersecurity Preparedness Act.

Sec. 2. The Legislature finds and declares that:

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

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

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

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

(5) 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 needs insight into the cybersecurity vulnerabilities of entities doing business with the state; and

(6) In addressing these issues, the office needs to establish strategic partnerships and contracts with companies that comply with state and federal cybersecurity standards.

Sec. 3. For purposes of the Cybersecurity Preparedness Act:

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

(2) Political subdivision means any village, city, county, school district, educational service unit, or natural resources district.

Sec. 4. The office shall:

(1) Support cybersecurity preparedness activities;

(2) Procure tools, hardware, software, or services that enhance or expand the state's cybersecurity defense and response capabilities. The

LB1302
2024

office shall ensure that contracts for such tools, hardware, software, or services permit access to the same pricing for any other state agency, including the Nebraska state colleges;

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

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

(5) Increase and maintain cyber incident response capabilities;

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

(7) Support cybersecurity workforce development within the state.

Sec. 5. The office shall develop an annual cybersecurity preparedness training activity to allow for hands-on defensive cyber training in an unclassified, closed-computing environment with the goals of:

(1) Protecting critical infrastructure from cyber threats by enhancing the interoperability between private industry leaders, the National Guard units from around the United States, international military partners, the United States Government, state governments, local governments, and nongovernmental organizations;

(2) Improving the understanding and capability to react to cyber incidents of different complexity and build partnerships that result in increased lines of communication and efforts to support Nebraska emergency management, critical infrastructure, and key resources;

(3) Conducting the following to prepare for simulated scenario-driven cyber attacks that require implementation of incident response plans and coordination of technical and administrative efforts:

(a) A live-fire cyber-exercise within a virtual training environment; and

(b) Preparatory academic coursework; and

(4) Allowing residents of Nebraska, cybersecurity leaders, and military service members to:

LB1302
2024

(a) Train in a joint environment;

(b) Enhance military readiness;

(c) Build partnerships; and

(d) Provide key services with lasting benefits to the State of Nebraska.

Sec. 6. The office shall 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:

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

(2) Notify each vendor that provides services to any state agency of any specific vulnerability relating to such vendor;

(3) Track the remediation efforts of each vendor that is determined to be of critical importance by the Chief Information Officer;

(4) Provide the office with software that provides the ability to query and track:

(a) Cyber threat actors; and

(b) Common vulnerabilities and exposures that are currently being weaponized and the ability to map such weaponized common vulnerabilities and exposures directly to the specific assets and threat actors within this state's vendor ecosystems, state agencies, and political subdivisions; and

(5) Provide political subdivisions the ability to monitor publicly observable cybersecurity vulnerabilities and vendor ecosystems.

Sec. 7. (1) The office shall create and administer a program to provide grants to political subdivisions for the purpose of upgrading critical information technology infrastructure.

(2) The office shall adopt and promulgate rules and regulations to

LB1302
2024

specify the eligibility criteria to receive a grant from the office under the program. At a minimum, the eligibility criteria shall require a political subdivision to specify how the grant will be used for the purposes described in subsection (4) of this section.

(3) The office shall prescribe the application form and the manner for submitting an application for a grant under this section.

(4) A political subdivision awarded a grant under this section shall use the grant only for the following purposes:

(a) Upgrading the critical information technology infrastructure of the political subdivision;

(b) Improving training on cybersecurity for agents of the political subdivision; and

(c) Working toward compliance with nationally recognized cybersecurity frameworks and other cybersecurity objectives outlined by the Chief Information Officer.

(5) The office may adopt and promulgate rules and regulations to carry out this section, including defining what qualifies as critical information technology infrastructure, setting parameters for cybersecurity training, selecting cybersecurity frameworks, and setting methods and metrics for determining the progress of a political subdivision toward compliance with such frameworks.

Sec. 8. The office shall purchase software and services, including 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 executive agencies of the state as long as the contracted software or services are offered to political subdivisions at no charge.

Sec. 9. When negotiating any contract under the Cybersecurity Preparedness Act, the office shall use vendors associated with existing

LB1302
2024

procurement contracts with the office to ensure an expedited purchasing process.

Sec. 10. (1) Except as provided in subsection (2) of this section, any party that contracts with the office for the sale of software or services under the Cybersecurity Preparedness Act shall:

(a) Be headquartered in the United States;

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

(c) Have achieved the ready stage in the Federal Risk and Authorization Management Program certification process.

(2) The office may contract with a party that does not satisfy the requirements specified in subsection (1) of this section only if no other party meets the requirements specified in subsection (1) of this section.

Sec. 11. The office may adopt and promulgate rules and regulations to carry out the Cybersecurity Preparedness Act.

Sec. 12. It is the intent of the Legislature to appropriate:

(1) Two million dollars each fiscal year for the purposes described in section 4 of this act, with up to one million dollars of such appropriation for expenditures for permanent and temporary salaries and per diems;

(2) One million dollars each fiscal year for the purposes described in section 5 of this act, with up to one million dollars of such appropriation for expenditures for permanent and temporary salaries and per diems;

(3) Four million dollars each fiscal year for the purposes described in section 6 of this act;

(4) Two million dollars each fiscal year for the purposes described in section 7 of this act, with up to five hundred thousand dollars of such appropriation for expenditures for permanent and temporary salaries and per diems; and

(5) Two million dollars each fiscal year for the purposes described in section 8 of this act, with up to two hundred fifty thousand dollars

LB1302
2024

of such appropriation for expenditures for permanent and temporary salaries and per diems.

Sec. 13. Since an emergency exists, this act takes effect when passed and approved according to law.