

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:

- 1 A BILL FOR AN ACT relating to cybersecurity; to adopt the Cybersecurity
- 2 Preparedness Act; and to declare an emergency.
- 3 Be it enacted by the people of the State of Nebraska,

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

3 Sec. 2. The Legislature finds and declares that:

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

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

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

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

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

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

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

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

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

28 Sec. 4. The office shall:

29 (1) Support cybersecurity preparedness activities;

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

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

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

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

7 (5) Increase and maintain cyber incident response capabilities;

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

9 and

10 (7) Support cybersecurity workforce development within the state.

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

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

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

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

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

29 (b) Preparatory academic coursework; and

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

- 1 (a) Train in a joint environment;
- 2 (b) Enhance military readiness;
- 3 (c) Build partnerships; and
- 4 (d) Provide key services with lasting benefits to the State of
- 5 Nebraska.

6 Sec. 6. The office shall secure and remediate the cybersecurity
7 vulnerabilities within the vendor ecosystems of vendors contracted with
8 the state, executive agencies, and political subdivisions by contracting
9 with a software provider that will:

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

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

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

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

20 (a) Cyber threat actors; and

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

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

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

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

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

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

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

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

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

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

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

22 Sec. 8. The office shall purchase software and services, including
23 identity access management, cybersecurity incident response capabilities,
24 cybersecurity training, and other activities that promote cybersecurity,
25 and make such software and services available to political subdivisions
26 at no cost. The Chief Information Officer may include services to be used
27 by the state and executive agencies of the state as long as the
28 contracted software or services are offered to political subdivisions at
29 no charge.

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

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

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

6 (a) Be headquartered in the United States;

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

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

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

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

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

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

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

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

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

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

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

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