H.291

Introduced by Representatives Sibilia of Dover and Chase of Colchester

Referred to Committee on

Date:

Subject: Executive; Agency of Digital Services; information technology; cybersecurity; critical infrastructure

Statement of purpose of bill as introduced: This bill proposes to statutorily create the Cybersecurity Advisory Council to advise on the State's cybersecurity infrastructure, standards, and safeguards. This bill also proposes to require the Cybersecurity Advisory Council to biennially review and approve the State's cybersecurity standards for the State's critical infrastructure domains.

An act relating to the creation of the Cybersecurity Advisory Council

It is hereby enacted by the General Assembly of the State of Vermont:

Sec. 1. 20 V.S.A. chapter 208 is added to read:

CHAPTER 208. CYBERSECURITY

§ 4661. DEFINITIONS

As used in this chapter:

(1) "Critical infrastructure" has the same meaning as in 11 V.S.A. § 1701.

(2) "Cybersecurity" means the practice of deploying people, policies, processes, and technologies to protect organizations, their critical systems, and sensitive information from digital attacks.

§ 4662. CYBERSECURITY ADVISORY COUNCIL

(a) Creation. There is created the Cybersecurity Advisory Council to advise on the State's cybersecurity infrastructure, standards, and safeguards.

(b) Membership. The Council shall be composed of the following members:

(1) one current member of the House of Representatives, who shall be appointed by the Speaker of the House;

(2) one current member of the Senate, who shall be appointed by the Committee on Committees;

(3) the Chief Information Officer, who shall serve as the Chair or appoint a designee from the Council to serve as the Chair;

(4) the Chief Information Security Officer;

(5) a representative from a State electrical public utility, appointed by the Governor;

(6) a representative from a State municipal water system, appointed by the Governor;

(7) a representative from a Vermont hospital or accountable care organization, appointed by the Governor;

(8) a person representing a Vermont business related to an essential supply chain, appointed by the Governor;

(9) the Director of Vermont Emergency Management or designee;

(10) the Governor's Homeland Security Advisor or designee;

(11) the Vermont Adjutant General or designee; and

(12) the Attorney General or designee; *and*

(13) the President of Vermont Information Technology Leaders or designee.

(c) Powers and duties. The Council shall have the following duties:

(1) develop a strategic plan for protecting the State's public sector and private sector information and systems from cybersecurity attacks;

(2) review and approve the State's cybersecurity standards for critical infrastructure domains;

(3) evaluate statewide cybersecurity readiness and develop best practices for policies and procedures to strengthen administrative, technical, and physical cybersecurity safeguards as a resource for State government, Vermont businesses, and the public;

(4) build relationships and conduct outreach within State government and to federal government and the private sector to ensure the resilience of electronic information systems;

(5) build strong partnerships with local universities and colleges in order to leverage cybersecurity resources; and

(6) identify and advise on opportunities to:

(A) ensure Vermont promotes, attracts, and retains a highly skilled cybersecurity workforce;

(B) raise citizen awareness through outreach and public service announcements;

(C) provide technical capabilities, training, and advice to local government and the private sector;

(D) provide recommendations on legislative action to the General Assembly to protect critical assets, infrastructure, services, and personally identifiable information;

(E) advise on strategic, operational, and budgetary impacts of cybersecurity on the State;

(F) engage State and federal partners in assessing and managing risk; and

(G) investigate ways the State can implement a unified cybersecurity communications and response.

(d) Assistance. The Council shall have the administrative and technical assistance of the Agency of Digital Services.

(e) Working groups and consultations.

(1) The Council may establish interagency working groups to support its charge, drawing membership from any State agency or department.

(2) The Council may consult with private sector and municipal, State, and federal government professionals for information and advice on issues related to the Council's charge.

(f) Meetings.

(1) The Chief Information Officer shall be the Chair of the Council.

(2) A majority of the membership shall constitute a quorum.

(3) The Council shall meet at least quarterly.

(g) Reports. On or before January 15 each year, the Council shall submit a written report to the House Committees on Commerce and Economic Development, on Environment and Energy, on Government Operations and Military Affairs, and on Ways and Means, and the Senate Committees on Economic Development, Housing and General Affairs, on Finance, and on Government Operations on information acquired pursuant to activities required under subsection (c) of this section and any recommendations for legislative action. The provisions of 2 V.S.A. § 20(d) (expiration of required reports) shall not apply to the report to be made under this subsection.

(b) Compensation and reimbursement.

(1) For attendance at meetings during adjournment of the General Assembly, a legislative member of the Council serving in the member's capacity as a legislator shall be entitled to per diem compensation and reimbursement of expenses pursuant to 2 V.S.A. § 23. These payments shall be made from monies appropriated to the General Assembly.

(2) Other members of the Council who are not otherwise compensated or reimbursed for their attendance shall be entitled to per diem compensation and reimbursement of expenses as permitted under 32 V.S.A. § 1010. These payments shall be made from monies appropriated to the Agency of Digital Services.

§ 4663. CYBERSECURITY STANDARDS FOR CRITICAL INFRASTRUCTURE

(a) Standards. Beginning on July 1, 2024 and biennially thereafter, the Cybersecurity Advisory Council, established pursuant to section 4662 of this title, shall review and approve the cybersecurity standards for the critical infrastructure domains. The standards shall include:

(1) the identification of critical infrastructure and the associated risks;

(2) the implementation of security controls to protect against identified risks;

(3) regular testing and evaluation of the effectiveness of the security controls;

(4) the development and implementation of incident response plans;

(5) the regular training of personnel on cybersecurity risks and incident response;

(6) the implementation of measures to protect against unauthorized access, use, disclosure, disruption, modification, or destruction of critical infrastructure data;

(7) compliance with all State and federal laws and regulations related to cybersecurity; and

(8) the implementation of measures to ensure the ongoing confidentiality, integrity, and availability of critical infrastructure.

(b) Standards for other regulatory bodies. The cybersecurity standards approved by the Council pursuant to subsection (a) of this section shall include:

(1) cybersecurity standards developed by the Public Utility Commission to protect the State's critical infrastructures relating to electric, water, telecommunications, and any other essential sectors as determined by the Commission.

(2) cybersecurity standards developed by the Green Mountain *Care* Board to protect the State's critical infrastructures relating to health care,

~~including hospitals, health care systems, accountable care organizations, and~~ other essential health systems as determined by the Board.

(c) Exemption. Any assessments and reports related to the cybersecurity standards for critical infrastructure are exempt from public inspection and copying under the Public Records Act and shall be kept confidential.

Sec. 2. 11 V.S.A. § 1701 is amended to read:

§ 1701. DEFINITIONS

~~In~~ As used in this chapter:

(1) "Critical infrastructure" means property and equipment owned or used by communications networks and electric generation, transmission, and distribution systems; water and wastewater systems; health systems; essential supply chains; and communications networks, including cellular, broadband, and telecommunications networks.

* * *

~~Sec. 3. EFFECTIVE DATE~~

~~This act shall take effect on July 1, 2023.~~

Sec. 3. REPEAL

20 V.S.A. chapter 208 (Cybersecurity) is repealed on June 30, 2026.

Sec. 4. EFFECTIVE DATE

~~This act shall take effect on July 1, 2023.~~

Sec. 1. 20 V.S.A. chapter 208 is added to read:

CHAPTER 208. CYBERSECURITY

§ 4661. DEFINITIONS

As used in this chapter:

(1) "Critical infrastructure" has the same meaning as in 11 V.S.A. § 1701.

(2) "Cybersecurity" means the practice of deploying people, policies, processes, and technologies to protect organizations, their critical systems, and sensitive information from digital attacks.

(3) "Essential supply chain" means supply chains for the production, in sufficient quantities, of the following articles:

(A) medical supplies, medicines, and personal protective equipment;

(B) articles essential to the operation, manufacture, supply, service, or maintenance of critical infrastructure;

(C) articles critical to infrastructure construction after a natural or manmade disaster;

(D) articles that are critical to the State's food systems, including food supplies for individuals and households and livestock feed; and

(E) articles that are critical to the State's thermal systems and fuels.

§ 4662. CYBERSECURITY ADVISORY COUNCIL

(a) Creation. There is created the Cybersecurity Advisory Council to advise on the State's cybersecurity infrastructure, best practices,

communications protocols, standards, training, and safeguards.

(b) Membership. The Council shall be composed of the following members:

(1) the Chief Information Officer, who shall serve as the Chair or appoint a designee from the Council to serve as the Chair;

(2) the Chief Information Security Officer;

(3) a representative from a distribution or transmission utility, appointed by the Commissioner of Public Service;

(4) a representative from a State municipal water system, appointed by Secretary of Natural Resources;

(5) a representative from a Vermont hospital, appointed by the President of the Vermont Association of Hospitals and Health Systems;

(6) a person representing a Vermont business related to an essential supply chain, appointed by the Chair of the Vermont Business Roundtable;

(7) the Director of Vermont Emergency Management or designee;

(8) the Governor's Homeland Security Advisor or designee;

(9) the Vermont Adjutant General or designee;

(10) the Attorney General or designee; and

(11) the President of Vermont Information Technology Leaders or designee.

(c) Powers and duties. The Council shall have the following duties:

(1) develop a strategic plan for protecting the State's public sector and private sector information and systems from cybersecurity attacks;

(2) evaluate statewide cybersecurity readiness and develop and share best practices for policies and procedures to strengthen administrative, technical, and physical cybersecurity safeguards as a resource for State government, Vermont businesses, and the public;

(3) build relationships and conduct outreach within State government and to federal government and the private sector to ensure the resilience of electronic information systems;

(4) build strong partnerships with local universities and colleges in order to leverage cybersecurity resources; and

(5) conduct an inventory and review of cybersecurity standards and protocols for critical sector infrastructures and make recommendations on whether improved or additional standards and protocols are necessary; and

(6) identify and advise on opportunities to:

(A) ensure Vermont promotes, attracts, and retains a highly skilled cybersecurity workforce;

(B) raise citizen awareness through outreach and public service announcements;

(C) provide technical capabilities, training, and advice to local government and the private sector;

(D) provide recommendations on legislative action to the General Assembly to protect critical assets, infrastructure, services, and personally identifiable information;

(E) advise on strategic, operational, and budgetary impacts of cybersecurity on the State;

(F) engage State and federal partners in assessing and managing risk;

(G) investigate ways the State can implement a unified cybersecurity communications and response, including recommendations for establishing statewide communication protocols in the event of a cybersecurity incident; and

(H) access cyber-insurance, including how to increase availability and affordability of cyber-insurance for critical industries.

(d) Assistance. The Council shall have the administrative and technical assistance of the Agency of Digital Services.

(e) Working groups and consultations.

(1) The Council may establish interagency working groups to support its charge, drawing membership from any State agency or department.

(2) The Council may consult with private sector and municipal, State, and federal government professionals for information and advice on issues related to the Council's charge.

(f) Meetings.

(1) A majority of the membership shall constitute a quorum.

(2) The Council shall meet at least quarterly.

(3)(A) In addition to 1 V.S.A. § 313, the Council is authorized to enter into an executive session to consider:

(i) testimony from a person regarding details of a cybersecurity incident or response to that incident, the disclosure of which would jeopardize public safety; or

(ii) any evaluations, recommendations, or discussions of cybersecurity standards, protocols, and incident responses, the disclosure of which would jeopardize public safety.

(B) Members of the Council and persons invited to testify before the Council shall not disclose to the public information, records, discussions, and opinions stated in connection to the Council's work if the disclosure would jeopardize public safety.

(g) Reports. On or before January 15 each year, the Council shall submit a written report to the House Committees on Commerce and Economic Development, on Environment and Energy, on Government Operations and Military Affairs, and on Ways and Means and the Senate Committees on Economic Development, Housing and General Affairs, on Finance, and on Government Operations with a status update on the work of the Council and

any recommendations for legislative action. The provisions of 2 V.S.A. § 20(d) (expiration of required reports) shall not apply to the report to be made under this subsection.

(h) Public records act exemption. Any records or information produced or acquired by the Council regarding cybersecurity standards, protocols, and incident responses, if the disclosure would jeopardize public safety, shall be kept confidential and shall be exempt from public inspection or copying under Vermont's Public Records Act. Notwithstanding 1 V.S.A. § 317(e), the Public Records Act exemption created in this section shall continue in effect and shall not be reviewed for repeal.

(i) Compensation and reimbursement. Members of the Council who are not otherwise compensated or reimbursed for their attendance shall be entitled to per diem compensation and reimbursement of expenses as permitted under 32 V.S.A. § 1010. These payments shall be made from monies appropriated to the Agency of Digital Services.

Sec. 2. 11 V.S.A. § 1701 is amended to read:

§ 1701. DEFINITIONS

~~In~~ As used in this chapter:

(1) "Critical infrastructure" means property and equipment owned or used by communications networks and electric generation, transmission, and distribution systems; water and wastewater systems; health systems; essential

supply chains; thermal fuels and systems; and communications networks, including cellular, broadband, and telecommunications networks.

* * *

Sec. 3. REPORT

On or before January 15, 2024, the Cybersecurity Advisory Council shall include in its report required by 20 V.S.A. § 4662(g) recommendations on whether to amend the definition of "essential supply chain", as defined in 20 V.S.A. § 4661, to include additional supply chains.

Sec. 4. REPEAL

20 V.S.A. chapter 208 (cybersecurity) is repealed on June 30, 2028.

Sec. 5. EFFECTIVE DATE

This act shall take effect on July 1, 2023.