HB 1728-FN - AS INTRODUCED

2026 SESSION

26-3165
07/06

HOUSE BILL ***1728-FN***

AN ACT requiring sufficient cybersecurity protections for critical infrastructure and technology projects.

SPONSORS: Rep. McFarlane, Graf. 18; Rep. Cambrils, Merr. 4; Rep. Popovici-Muller, Rock. 17; Rep. Sabourin dit Choiniere, Rock. 30; Rep. Vose, Rock. 5; Rep. Wheeler, Hills. 33; Sen. Pearl, Dist 17

COMMITTEE: Science, Technology and Energy

ANALYSIS

This bill seeks to establish a statutory "standard of care" for operators of critical infrastructure technology systems serving large populations in New Hampshire.

- -

Explanation: Matter added to current law appears in ***bold italics.***
Matter removed from current law appears [~~in brackets and struckthrough.~~]
Matter which is either (a) all new or (b) repealed and reenacted appears in regular type.

26-3165
07/06

STATE OF NEW HAMPSHIRE

In the Year of Our Lord Two Thousand Twenty-Six

AN ACT requiring sufficient cybersecurity protections for critical infrastructure and technology projects.

Be it Enacted by the Senate and House of Representatives in General Court convened:

1 Statement of Findings. The general court hereby finds that:

I. New Hampshire recognizes a duty to exercise reasonable care under all circumstances to prevent foreseeable harms.

II. Certain operational technology systems, if configured or maintained without due care, create foreseeable and unreasonable risks, not only to operators, but to entire communities and our national defense.

III. Public health, safety, and welfare requires heightened attention where failures to certain operational technology systems could cause material disruptions or harms to large numbers of people.

2 New Chapter; Critical Infrastructure Technology Practices. Amend RSA by inserting after chapter 546-C the following new chapter:

CHAPTER 546-D

CRITICAL INFRASTRUCTURE TECHNOLOGY PRACTICES

546-D:1 Definitions.

I. As used in this chapter, "critical infrastructure operational technology" means the control systems, central operator-machine interfaces, and related components that directly support the provision of essential services, including drinking water supply, treatment and distribution systems, wastewater collection and treatment systems, electric power generation, transmission and distribution systems, natural gas transmission and distribution systems, communications systems, emergency response systems, and public transportation systems.

II. For purposes of this chapter, the use of Internet or cloud services solely for logging, telemetry or archival functions, including cybersecurity detection and analysis, shall not constitute “continued safe operation.”

546-D:2 Standard of Care.

I. Operators of critical infrastructure operational technology systems serving more than 10,000 people or 3,300 households within this state shall exercise reasonable care under all the circumstances to secure such systems against foreseeable risks, including those arising from:

(a) Direct exposure of controls, interfaces, or human-machine interfaces to the public Internet or other public networks without the interposition of firewall technologies which enforce

inbound and outbound access permissions, allowing only specific access for documented reasons and denying all other access by default;

(b) Indirect exposure through remote access solutions, including but not limited to dial-up, cellular modem, and Internet virtual private networks, that do not enforce phishing-resistant multi-factor authentication controls;

(c) Lack of methods to temporarily terminate and disable remote access sessions and capabilities, including interactive and system-to-system remote access;

(d) Failure to reasonably maintain and patch firewalls and remote access systems;

(e) Lack of a cybersecurity incident response and recovery plan; and

(f) Dependence upon uninterrupted access to Internet or cloud services for continued safe operation and function of the supported critical infrastructure service.

II. An operator who fails to exercise reasonable care under this section shall be liable for harms proximately caused by such failure. In determining liability, the magnitude of risk to public health and safety, the burden of taking precautions, and the degree to which the hazard was reasonably foreseeable shall be considered.

3 Effective Date. This act shall take effect January 1, 2027.

LBA
26-3165
12/12/25

HB 1728-FN- FISCAL NOTE
AS INTRODUCED

AN ACT requiring sufficient cybersecurity protections for critical infrastructure and technology projects.

FISCAL IMPACT: This bill does not provide funding, nor does it authorize new positions.

Estimated Political Subdivision Impact				
	FY 2026	**FY 2027**	**FY 2028**	**FY 2029**
County Revenue	$0	$0	$0	$0
County Expenditures	$0	Indeterminable Increase		
Local Revenue	$0	$0	$0	$0
Local Expenditures	$0	Indeterminable Increase		

METHODOLOGY:

This bill establishes a statutory standard of care for operators of critical infrastructure operational technology systems serving more than 10,000 people or 3,300 households. Operators must exercise reasonable care to secure essential services against foreseeable risks. Failure to meet this standard may result in liability for resulting harms.

The Department of Administrative Services (DAS) reports that the Division of Risk and Benefits previously purchased cybersecurity insurance, but the rising costs made it unsustainable. In response, the Department of Information Technology (DoIT) implemented a self-insurance program in 2022. As a result, DAS indicates there will be no fiscal impact from this bill, since the state no longer purchases cybersecurity insurance.

The Department of Information Technology indicates that they do not manage or regulate critical infrastructure systems, and any costs associated with implementing the legislation would fall on the infrastructure entities.

The New Hampshire Municipal Association (NHMA) states that municipalities operating such infrastructure may incur indeterminable costs ranging from $100,000 to $500,000 due to any necessary technology upgrades. Larger cities may see a higher cost.

The New Hampshire Association of Counties (NHAC) indicates that while the bill allows for litigation, the fiscal impact is currently indeterminable due to the unpredictability of legal costs.

AGENCIES CONTACTED:

Department of Administrative Services, Department of Information Technology, New Hampshire Municipal Association, and New Hampshire Association of Counties