The Institute of Internal Auditors
Elevating Impact

June 24, 2024

Honourable Ron McKinnon, Member of Parliament
Standing Committee on Public Safety and National Security, Chair
Sixth Floor, 131 Queen Street
House of Commons
Ottawa ON K1A 0A6

RE: IIA Comments on the Critical Cyber Systems Protection Act (Bill C-26, Part II)

Dear Mr. McKinnon,

On behalf of The Institute of Internal Auditors (The IIA), the international professional association representing over 245,000 internal auditors, with members across Canada, we appreciate the opportunity to comment on the House of Commons' proposed legislation entitled: *Critical Cyber Systems Protection Act* (Bill C-26, Part II).

According to a recent survey of chief audit executives published by The IIA, 78% of respondents acknowledged that cybersecurity constituted a "high" or "very high" risk to their organization.[1] As companies from all industries and sectors confront a dynamic cybersecurity risk environment, it is evident a robust legislative/regulatory framework is necessary to accomplish two primary objectives:

- Institute processes for effectively identifying and mitigating potential organizational cybersecurity risks
- Establish appropriate internal controls and independent assurance procedures

Due to the internal audit profession's central role in evaluating cybersecurity risk, The IIA commends the Standing Committee on Public Safety and National Security (Standing Committee) for its continued leadership on this important policy issue. The application of consistent cybersecurity regulatory processes – especially among federally regulated sectors – has the potential to enhance organizational defences and promote greater consumer protections.[2]

The proposed *Critical Cyber Systems Protection Act* authorizes multiple governmental officials – such as the Superintendent of Financial Institutions and Minister of Industry – to order an internal audit at a designated operator regulated pursuant to this legislation. Each reference to a government-directed internal audit order states the following:

> *…order a designated operator to, within a specified period and in accordance with the order, conduct an internal audit of its practices, books and other records to determine whether the designated operator is in compliance with any provision of this Act or the regulations.*[3]

Upon a comprehensive review of the relevant provisions, The IIA believes one technical clarification is merited. Although the proposed legislation implies the internal audit function at a designated operator is responsible for conducting these evaluations, the bill remains silent on the processes and procedures governing "how" such an audit shall be performed.

Given the complexity of evaluating cybersecurity risk and compliance – and the need for such an

[1] "2023 North American Pulse of Internal Audit: Benchmarks for Internal Audit Leaders," *The Institute of Internal Auditors*, March 2023
[2] The Government of Canada's Directive on Internal Audit also establishes robust internal audit functions within departments which can be used to support critical infrastructure-related organizations.
[3] "Critical Cyber Systems Protection Act (Bill C-26, Part II)," House of Commons of Canada, amended April 19, 2024

The Institute of Internal Auditors
Elevating Impact

evaluation to be performed objectively – it is imperative that the Standing Committee define an audit framework designed to promote consistent execution. To achieve this objective, The IIA proposes inserting a narrow clause in each relevant subsection authorizing an internal audit so the text reads:

> *…order a designated operator to, within a specified period and in accordance with the order, conduct an internal audit – in conformity with globally recognized internal auditing standards – of its practices, books and other records to determine whether the designated operator is in compliance with any provision of this Act or the regulations…*

The incorporation of this technical reference will minimize potential audit ambiguity and engender organizational confidence through indirect:

- Establishment of organizational reporting relationships that promote audit independence and objectivity
- Identification of required certifications or credentials necessary to perform the internal audit
- Reference to the relevant professional standards to which internal auditors must comply in performance of their duties

Should you or your staff have any questions regarding this matter or wish to discuss ways in which the internal audit profession can support your work, please contact Jillian Fernandez, Director, Advocacy (Canada), at jillian.fernandez@theiia.org.

Thank you for your consideration of our comments.

Sincerely,

Anthony J. Pugliese, CIA, CPA, CGMA, CITP
President and Chief Executive Officer
The Institute of Internal Auditors

Jeff McIlravey, CRMA, CFSA
Director, Canada
The Institute of Internal Auditors

cc: Members of the Standing Committee on Public Safety and National Security