



August 14, 2023

The Honorable Adrienne A. Harris
New York Department of Financial Services
One State Plaza
1 State Street
New York, NY 10004

RE: IIA Comments Regarding “Revised Proposed Second Amendment to 23 NYCRR 500”

Dear Superintendent Harris:

On behalf of The Institute of Internal Auditors (The IIA), the international professional association representing over 235,000 internal auditors, I appreciate the opportunity to comment on the New York Department of Financial Services’ (NYDFS) revised regulatory proposal entitled: “[Cybersecurity Requirements for Financial Services Companies](#).”

According to a recent survey of chief audit executives published by The IIA, cybersecurity was identified as the number one risk currently confronting organizations.¹ As companies from all industries and sectors confront a dynamic cybersecurity risk environment, it is evident a robust 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 NYDFS for its continued leadership on this important policy issue. The application of consistent cybersecurity regulatory processes – specifically with respect to financial services – has the potential to enhance organizational defenses and promote greater consumer protections.

The revised cybersecurity proposal, published by NYDFS on June 28, 2023, represents the next important step in cultivating a sound regulatory posture. While the updated version includes a series of new provisions and modifications, The IIA specifically applauds the insertion of “internal audit” into the definition of “independent audit.”

As The IIA argued in a letter to NYDFS, dated January 9, 2023, covered entities must preserve the “option” of utilizing an internal audit function to perform any required independent audits.² The revised proposal embraces The IIA’s recommendation and appropriately positions internal audit as a pivotal resource in evaluating and combatting cybersecurity risk.

Upon further review of the revised “independent audit” definition, however, The IIA believes an additional technical clarification is merited. Although the updated proposal outlines “who” may conduct

¹ “2023 North American Pulse of Internal Audit: Benchmarks for Internal Audit Leaders,” *The Institute of Internal Auditors*, March 2023

² “Comments to the Proposed Second Amendment to 23 New York Codes, Rules, and Regulations (NYCRR) Part 500 (Part 500),” *The Institute of Internal Auditors*, January 9, 2023

an independent audit (i.e. internal and external auditors), the regulation remains silent on the processes and procedures governing “how” such an audit shall be performed.

Given the complexity of evaluating cybersecurity risk, it is imperative that NYDFS define an audit framework designed to promote consistent application of the regulation. The IIA contends incorporating such technical guidance into Section 500.1(g) will minimize potential audit ambiguity and engender organizational confidence through:

- Specific definitions clarifying the differences between internal and external audit
- Establishment of organizational reporting relationships that promote audit independence and objectivity
- Identification of required certifications or credentials necessary to perform an independent audit
- References to relevant laws, regulations, or professional standards to which internal and external auditors must comply in performance of their duties

For example, The IIA believes insertion of the following language as Section 500.1(g)(1) will provide internal auditors sufficient technical information to appropriately conduct an independent audit³:

(1) INTERNAL AUDIT.— The term “internal audit” means a professional individual or group within a covered entity who, in conformity with globally accepted internal auditing standards, is responsible for providing: the board of directors, an audit committee, if applicable; and management with: objective assurance over the covered entity’s internal controls; consulting services; and with strategic advice on risk mitigation. For the purposes of this Regulation, internal audit shall be—

(i) Independent from management, reporting to the entity’s board of directors, a committee, or another body to which the board of directors has delegated certain functions;

(ii) Led by a qualified professional responsible for effectively managing all aspects of the internal audit function and ensuring the quality performance of internal audit services;

(a) The leader of the internal audit function, and relevant staff, shall hold:

(I) appropriate professional certifications or other credentials, such as the Certified Internal Auditor credential;

(II) or specialty credentials related to expertise in cybersecurity.

(b) No provision in this Regulation shall exclude the option of a partially or fully outsourced internal audit function, provided the entity fulfilling the internal audit function does not provide external audit services to the same covered entity.

(iii) Required to establish a written internal audit charter agreed upon by both the board of directors and the qualified professional leading the internal audit function.

³ NOTE: The IIA also recommends the insertion of a similar clarifying definition for “external audit” as Section 500.1(g)(2).

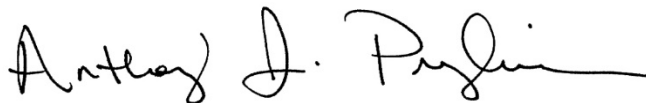
Since cybersecurity risk is omnipresent and rapidly evolving, NYDFS must balance the need for prescriptive regulations with preserving innovation and flexibility. In essence, The IIA's proposed insertion of Section 500.1(g)(1) accomplishes this dual objective by:

- Explicitly instructing internal auditors to perform an independent audit in conformity with globally accepted internal auditing standards
- Tacitly embracing any future standards or guidance published by The IIA intended to enhance internal audits of cybersecurity risk and internal controls

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 Alex Sload, IIA Senior Manager for Advocacy and State Policy, at Alex.Sload@TheIIA.org.

Thank you for your consideration of our comments.

Sincerely,

A handwritten signature in black ink that reads "Anthony J. Pugliese". The signature is written in a cursive, flowing style.

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