The Institute of Internal Auditors
Elevating Impact

January 9, 2023

Adrienne A. Harris, Superintendent of Financial Services
The New York State Department of Financial Services
One State Plaza
1 State Street
New York, NY 10004-1511

RE: Comments to the Proposed Second Amendment to 23 New York Codes, Rules, and Regulations (NYCRR) Part 500 ("Part 500").

Dear Ms. Harris,

The Institute of Internal Auditors (IIA) appreciates the opportunity to share comments on your pending Proposed Second Amendment to 23 NYCRR 500. As the President and CEO of The IIA, I am proud to represent a global association of over 218,000+ members located in 170 countries around the world. For over 80 years, The IIA has aided sound governance and risk management efforts in public- and private-sector organizations, encouraging strong internal controls and an enterprise-wide approach. Auditing information systems and security is top of mind for practitioners and policymakers in this age of digital transformation and disruption, and we know from The IIA's OnRisk 2022[1] survey that cybersecurity remains the ***top*** risk identified by chief audit executives, boards of directors, and C-suite executives.

We applaud the State of New York for adopting Part 500, the first-of-its-kind mandatory state cybersecurity and risk management regulations for "covered entities"[2] in 2017. Since their development, these regulations have served as a valuable reference for other cybersecurity regulatory bodies in other jurisdictions. The proposed updates to these regulations, now out for public comment, further reflect the critical proactive engagement of the Department to stay on the forefront of cybersecurity. However, we have serious concerns about the Department's proposed amendment to the definition of independent audit as modified and released on November 9, 2022.

More specifically, in response to your request for comments, we offer the following feedback and suggestions.

[1] OnRisk 2022: A Guide to Understanding, Aligning and Optimizing Risk LINK
[2] Part 500 defines Covered Entities as persons operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law.

The Institute of Internal Auditors
Elevating Impact

Presently, as you are aware, audit is not defined in the existing regulations. The regulation also does not specify who should conduct an audit, its basic deliverables, which can vary substantially, and who in the organization should engage an external audit or additional audit resources when needed.

The first draft of the Proposed Amendments released in July of 2022 added, under Section 500.2 Cybersecurity Program, the following independent audit requirement:

> (c) Class A companies shall conduct an independent audit of their cybersecurity programs at least annually.

Additionally, the proposal included a definition of independent audit under xsection 500.1:

> (f) *Independent audit* means an audit conducted by auditors free to make their decisions, not influenced by the covered entities being audited or by its owners, managers, and employees. Such an audit can be conducted by auditors internal or external to the covered entity and its affiliates.

However, the latest proposed amendment language, released in November 2022, has now altered the previously proposed definition of independent audit to ***exclude*** an internal audit function from conducting this independent audit:

> (f) *Independent audit* means an audit conducted by external auditors free to make decisions not influenced by the covered entities being audited or by its owners, managers or employees.

We believe that it would be a grave mistake to remove the ***option*** to have an independent audit performed by covered entities' internal audit function. Rather, we would argue more forcefully that it should actually be a ***requirement*** for covered entities - an essential corporate governance best practice critical to the successful operations of all covered entities.

The internal audit function, operating in conformance with the IIA's *Standards*, is best positioned to provide an independent audit, providing a holistic assessment of and objective assurance over specific risk and risk management effectiveness.

Internal audit functions, when properly structured, are inherently independent, reporting to their governing bodies, often through an audit or risk committee, comprising independent directors of the board. Such requirements in IIA *Standards* ensure that the internal audit function operates independent of executive management and that internal auditors are not unfairly influenced or compromised by management.

The Institute of Internal Auditors
Elevating Impact

The independent role and value proposition of the internal audit function is best articulated in The IIA's Three Lines Model (3LM). The 3LM clarifies specific roles and responsibilities among an organization's leadership (e.g., governing body, management, and internal audit function) to promote strategic and operational alignment, proper oversight, and independence of the internal audit function. As such, again, I'd like to underscore that we believe that an independent audit performed by an internal audit function should be ***mandatory*** in the proposed regulations.

By design, internal auditors provide a broad, holistic view of the operations of an organization looking not just at an organization's financials, but also at key strategic and operational risks such as cybersecurity, data privacy and security, fraud, supply chain management, political and legal risks, and long-term strategy. They are in-house experts focused every day on adding value and supporting risk management throughout the entire organization. Such a powerful perspective is unique in comparison to other forms of audit where an external auditor comes in to examine retrospectively what already happened.

Proposed Updates to the Pending Regulation:
Considering internal auditors' expertise, special insight, and established independence, we would suggest that Section 500.2 (c) be rewritten as the following:

> (c) Class A companies shall conduct an independent internal audit of their cybersecurity programs at least annually.

Subsequently, we would include a new definition of *independent internal audit* under section 500.1 in lieu of a definition of *independent audit*:

> (f) *Independent internal audit* means an audit conducted by a covered entity's internal audit function.

Furthermore, to ensure that covered entities' internal audit functions are operating properly and are truly structured as independent, we would also suggest that a definition for "internal audit function" be added to the regulations.

In the appropriate place insert and renumber accordingly:

> ( ) *Internal audit function*.— The term "internal audit function" 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 strategic advice on risk mitigation. For the purposes of this Regulation, an internal audit function shall be—

A. 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;

B. 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;

(i) 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; or

(II) specialty credentials related to expertise in cybersecurity.

(ii) 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.

C. 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.

This proposed definition of *internal audit function* is designed to encompass core principles found in the Three Lines Model, including ensuring independence (i.e., direct reporting to the board of directors or its audit committee) and competency, while also allowing for flexibility when warranted. Different covered entities, as directed by their boards of directors, may come to different conclusions about how best to establish and support their internal audit functions. Of particular note, some internal audit functions may include outsourced or co-sourced audit services, which are permissible as long as such services don't present a conflict of interest and such services are engaged and overseen appropriately by the board of directors, its audit committee, and/or the leader of the internal audit function.

The Institute of
Internal Auditors
Elevating Impact

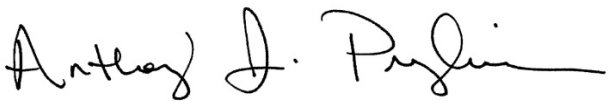
Upon codifying a mandatory internal audit requirement in regulation, the Department may also conclude that there would be additional value in having an external audit firm perform a supplemental audit of covered entities. Such a frequency for this type of audit may be annual or may be on a less frequent basis depending on an analysis of the costs and benefits.

We would defer to the Department on the necessity, appropriateness, and frequency of such a requirement. We would note, however, that, if the Department does determine that it is in the public interest to require a supplemental audit through an external audit firm, it is critical to ensure that that audit engagement is also structured to ensure objectivity and independence. In such cases, the external audit firm, like an internal audit function, should report solely to the governing body or the audit committee and the engagement should be overseen by the internal audit function as part of an outsourcing arrangement or a separate coordinated engagement. The cybersecurity program review should not be engaged and overseen by executive management.

Regardless of whether the Department were to mandate a supplemental external audit or not, we are confident that our proposed changes would help advance the Department's goals of protecting stakeholders and advancing the public interest by creating an independent audit requirement for cybersecurity programs.

I want to thank you for the opportunity to comment on the Department's proposal. Should you or your staff have any questions regarding our suggestions or if you would like to discuss the proposal in greater detail, I would ask you to please contact Mat Young, IIA Vice President for Global Advocacy, Policy, and Government Affairs, Mat.Young@theiia.org.

Sincerely,



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