

April 7, 2025

The Honorable Brett Guthrie
U.S. House Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515

RE: IIA Comments Regarding the Development of a Data Privacy and Security Framework

Dear Chairman Guthrie:

On behalf of The Institute of Internal Auditors (The IIA), the international professional organization representing more than 260,000 internal auditors, I appreciate the opportunity to comment on the House Committee on Energy and Commerce's (Committee) request for information regarding the development of a data privacy and security framework.

It is clear that the expansion of technological innovation has fundamentally transformed the lives of all Americans. The rapid acceleration of technology has facilitated instantaneous global communication, increased access to information, and contributed to the rise of a multi-trillion-dollar digital economy.¹ Unlike traditional security and commodity markets, this evolving digital economy is primarily driven by a new form of currency: **consumer data**.

The wealth of available consumer information – particularly over the last decade – has enabled companies, in part, to create individualized commercial and entertainment experiences. Through algorithms and other proprietary technologies, consumers regularly receive personalized and integrated online recommendations that include:

- Filtered search engine results
- Targeted retail advertisements
- Recommended local restaurants and travel destinations

Although the prevalence of data promotes greater convenience for American consumers, it also substantially increases risk through data breaches, privacy violations, and other cybercrimes. According to a recent IBM report, "the global average cost of a data breach in 2024" was \$4.8 million. Moreover, the data revealed approximately 33% of breaches "[show] the proliferation of data is making it harder to track and safeguard."²

To combat the risk of unauthorized data disclosures, The IIA believes it is imperative that any data privacy and security framework **encourage organizations to maintain an independent internal audit function**.

¹ U.S. House Committee on Energy and Commerce. (February 21, 2025). *Chairman Guthrie and Vice Chairman Joyce Issue Request for Information to Explore Data Privacy and Security Framework* [Press Release].
<https://energycommerce.house.gov/posts/chairman-guthrie-and-vice-chairman-joyce-issue-request-for-information-to-explore-data-privacy-and-security-framework>

² IBM. (2024). *Cost of a Data Breach Report 2024*. <https://www.ibm.com/reports/data-breach>

As you may know, an internal audit function – operating in conformity with the [Global Internal Audit Standards](#) – is the entity responsible for providing an organization’s governing body (i.e. board of directors) with objective assurance over data privacy-related risk management and internal control processes. In other words, internal audit leverages a deep understanding of the organization to conduct evaluations designed to promote data security and accountability. This private-sector approach to oversight is important because it ensures the professionals performing assessments possess a thorough knowledge of the organization’s strategic goals, culture, processes, and risk appetite. These powerful insights produce audits that provide a governing body with substantive and actionable information.

Recent congressional efforts regarding data privacy and online safety have tacitly embraced the core principles of internal audit; however, the terms used to describe the process are often technically imprecise. For example, the proposed *Kids Online Safety Act (KOSA)* – introduced by Senator Marsha Blackburn and Senator Richard Blumenthal during the 118th Congress – illustrates a commonly adopted legislative approach:

*...a covered platform shall issue a public report describing the reasonably foreseeable risks of material harms to minors and assessing the prevention and mitigation measures taken to address such risk based on an **independent, third-party audit** conducted through reasonable inspection of the covered platform,³ (emphasis added).*

The duties prescribed in this subsection of *KOSA* represent the **foundation of internal audit**. The profession helps “an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.”⁴ Although internal audit is the appropriate entity to perform data privacy and online safety evaluations, lawmakers often assign this responsibility to a third-party auditor.

While this paradigm is ostensibly intended to promote independence since the auditor is external to an organization, it obscures several important characteristics of third-party audit and internal audit:

- Both a third-party auditor and internal auditor functionally report to an organization’s governing body; therefore, internal audit is no less independent than a contracted third-party auditor
- Third-party audits traditionally conduct evaluations based upon a defined timeline (i.e. activities/operations over the last year, etc.)
- Internal audit performs continuous organizational assessments of high-risk programs and/or operations

Given the significant financial and reputational costs of data privacy violations in an increasingly connected digital economy, it is essential that Congress implement commonsense solutions to protect American consumers. The presence of an organizational internal audit function – consistent with prior legislative intent – can properly facilitate private sector-based transparency and accountability. Internal audit not only supplies the governing body with objective assurance on the effectiveness of controls and systems, but it also provides consumers with confidence that data is securely stored and appropriately utilized.

³ Kids Online Safety Act, S. 1409, 118th Congress (2023). <https://www.congress.gov/bill/118th-congress/senate-bill/1409/text>

⁴ The Institute of Internal Auditors. *What is Internal Auditing?* <https://www.theiia.org/en/about-us/about-internal-audit/>

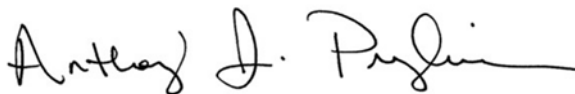
It is for this reason that The IIA recommends the Committee consider the following important topics when developing a new data privacy and security framework:

- 1) **Strengthen Internal Data Privacy Oversight:** Encourage internal audit-led assurance processes for evaluating an organization's data privacy-related internal controls, risk management and governance structures. The presence of a qualified internal audit function will strengthen independent oversight efforts and increase consumer confidence.
- 2) **Recognize the Distinction Between Internal Audit and Third-Party Audit:** Acknowledge that internal audit is the independent entity responsible for the assessment of organizational data privacy risk. Internal audit supplies a continuous evaluation of processes rather than the retroactive analysis performed by third-party audit.

Should the Committee have any questions regarding these comments, or wish to receive a briefing on the internal audit profession, please contact Michael Downing, IIA Senior Director for North American Advocacy, at Michael.Downing@TheIIA.org.

Thank you for your consideration of our comments.

Sincerely,

A handwritten signature in black ink, reading "Anthony J. Pugliese". The signature is fluid and cursive, with the first name "Anthony" and last name "Pugliese" clearly legible.

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

cc: The Honorable John Joyce, M.D.
Vice Chairman
U.S. House Committee on Energy and Commerce