The Institute of Internal Auditors
Elevating Impact

June 11, 2026

The Honorable Gus Bilirakis
Chair
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
U.S. House of Representatives

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce, Manufacturing, and Trade
Committee on Energy and Commerce
U.S. House of Representatives

Re: The Institute of Internal Auditors' (The IIA) Comment on H.R. 8413, the Securing and Establishing Consumer Uniform Rights and Enforcement over Data Act (SECURE Act)

Dear Chair Bilirakis and Ranking Member Schakowsky:

On behalf of The Institute of Internal Auditors (The IIA), I respectfully submit this letter in connection with the Subcommittee on Commerce, Manufacturing, and Trade's June 3, 2026, hearing examining legislation to establish a federal data privacy and security law.

The IIA is the internal audit profession's global standard-setting body, certification authority, and principal advocate. We represent more than 265,000 members worldwide, including over 75,000 in North America. The IIA administers the International Professional Practices Framework® (IPPF®), the authoritative standards and guidance used by internal auditors to provide independent, objective assurance and advisory services. Internal auditors operate independently inside the organizations they serve and report directly to the board or its audit committee. This reporting relationship uniquely positions internal audit to evaluate whether an organization's controls, including those governing the privacy and security of personal data, are designed appropriately and operating as intended.

The IIA has long advocated for the enactment of strong data privacy and security laws that that recognizes the importance of an internal audit function in minimizing the risk of non-compliance and internal control failures.[1] We write to underscore a point central to the durability of any data privacy and security regime: statutory requirements protect consumers and the public only when organizations can demonstrate that the controls designed to meet those requirements are functioning effectively in practice. Independent assurance provides that confidence.

I. The Role of Independent Internal Assurance

Section 4 of H.R. 8413 would require covered entities to establish and maintain a comprehensive data security program "that reasonably conforms to a relevant Federal or

[1] The IIA, Public Policy: Data Privacy & Security, *https://www.theiia.org/en/about-us/advocacy/* (last visited June 3, 2026).

widely accepted international risk management framework for identifying and protecting against data security risks, and for detecting, responding to, and recovering from data security events." We respectfully observe that requiring a documented risk management program does not guarantee a functioning system in practice. The mechanism that bridges the gap is independent internal assurance, which gives boards, regulators, and ultimately consumers, confidence that controls are operating effectively over time.

This is the role the internal audit profession is structured to perform. Under The IIA's Three Lines Model:

- Management owns and operates controls (first-line)
- Risk and compliance functions monitor them (second-line)
- Internal audit provides independent and objective assurance on the adequacy and effectiveness of governance, risk management, and control (third-line); further, internal audit reports its findings directly to the board or its audit committee.[2]

The independence that governs internal audit is established through accountability to the governing body, unfettered access to the people and data needed to do the work, and freedom from interference. This is a key characteristic that distinguishes internal audit's assurance from management's own self-assessment.

Critically, the profession already maintains authoritative guidance mapped to meet the very obligations Section 4 would impose. The IIA's Global Technology Audit Guides direct internal auditors in assessing cybersecurity risk and in evaluating an organization's ability to detect, respond to, and recover from cyber incidents in alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.[3] In 2025, The IIA elevated these expectations further by issuing a Cybersecurity Topical Requirement—a component of the IPPF® that establishes a mandatory baseline for assessing the design and implementation of cybersecurity governance, risk management, and control processes.[4] The tools designed to provide credible, independent assurance over the programs this bill contemplates, therefore, already exist and are in active use across the economy.

II. Recommendations for the Subcommittee's Consideration

As the Subcommittee refines this legislation, The IIA respectfully offers the following observations:

First, any data privacy and security legislation should preserve a flexible, framework-based approach of the kind reflected in Section 4 of H.R. 8413. Anchoring obligations to widely accepted risk management frameworks promote consistency, scalability across

[2] The IIA, *The IIA's Three Lines Model: An Update of the Three Lines of Defense* 4 (July 2020).

[3] The IIA, *Global Technology Audit Guide (GTAG): Assessing Cybersecurity Risk—The Three Lines Model* (Sept. 2020); The IIA, *GTAG: Auditing Cyber Incident Response and Recovery* (2d ed. 2024) (mapping internal audit procedures to the NIST Cybersecurity Framework "respond" and "recover" functions).

[4] The IIA, *Cybersecurity Topical Requirement* (Feb. 5, 2025) (a mandatory component of the IPPF® establishing a baseline for assessing the design and implementation of cybersecurity governance, risk management, and control processes).

organizations of differing size and complexity, and interoperability with the controls structures that responsible entities already maintain.

Second, any comprehensive federal privacy framework Congress enacts should provide for an independent internal audit function to deliver assurance over a covered entity's data security program.[5] Independent assurance ensures that compliance is demonstrated not merely by adopting a written policy, but by independently verifying that controls are designed appropriately and operating as intended—the hallmark of a mature and effective program.

Third, any final legislation should recognize that the independent internal audit function contemplated in the preceding recommendation derives its credibility from conformance with an established professional framework. As noted above, the IPPF® is the principal framework for the internal audit profession in the United States and internationally, and assurance performed in conformance with it provides Congress, regulators, and covered entities a common, recognized basis on which to rely.

III. Conclusion

The IIA shares the Subcommittee's goal of a clear, enforceable national standard that gives Americans meaningful control over their personal data while supporting continued innovation. The sustained, deliberative work that produced this hearing represents an important contribution to a long-overdue national conversation on consumer privacy. We respectfully encourage the Subcommittee to ensure that any final legislation accounts not only for what organizations must do to protect personal data, but for how compliance with those obligations can be independently verified and sustained over time. The internal audit profession stands ready to serve as a resource to the Subcommittee and its staff as this legislation advances.

Thank you for the opportunity to submit these views. Should you or your staff have any questions regarding our recommendations or if you would like to discuss this matter in greater detail, please have your staff contact Ramón A. Correa, IIA Director for U.S. Advocacy at Ramon.Correa@TheIIA.org.

Sincerely,

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

cc: The Honorable Brett Guthrie, Chairman, Committee on Energy & Commerce
The Honorable Frank Pallone, Jr., Ranking Member, Committee on Energy & Commerce

[5] Internal Audit Foundation, *Privacy and Data Protection, Part 1: Internal Audit's Role in Establishing a Resilient Framework* (2024).