



March 22, 2023

The Honorable Cathy McMorris Rodgers  
United States House of Representatives  
2188 Rayburn House Office Building  
Washington, DC 20515

The Honorable Frank Pallone, Jr.  
United States House of Representatives  
2107 Rayburn House Office Building  
Washington, DC 20515

***RE: IIA Proposed Amendments to the American Data Privacy and Protection Act***

Dear Chairwoman McMorris Rodgers and Ranking Member Pallone:

On behalf of the Central Jersey and Spokane Chapters of The Institute of Internal Auditors (The IIA), the international professional association representing approximately 1,800 internal auditors in New Jersey and Washington, we write to encourage consideration of new provisions designed to strengthen corporate governance and internal controls related to data privacy and security.

In 2022, thanks to your joint leadership, the U.S. House of Representatives was poised to adopt one of the most significant consumer protection laws in more than a generation. The American Data Privacy and Protection Act (ADPPA) would have established, for the first time, a uniform data privacy legal and regulatory framework intended to grant consumers authority over their online data.

Although the ADPPA substantially advanced debate concerning data privacy and security, the legislation did not acknowledge the importance of effective corporate governance and internal controls in minimizing online consumer data risks.

Our chapters believe it is imperative for organizations – specifically those involved in collecting and processing consumer data – to possess a clearly defined governance structure, including an internal audit function within the organization, identifying excessive risk and potential internal control failures. Such a paradigm helps ensure sound business operations, strengthens consumer protections, and best serves the public interest.

In January, The IIA transmitted to your personal offices, and the Subcommittee on Innovation, Data, and Commerce, a memorandum highlighting several proposed enhancements to the ADPPA. In short, the proposed modifications increase consumer protections by bolstering objective assurance over corporate governance and internal controls related to data privacy and security. The IIA believes inclusion of internal audit in certain sections of the ADPPA will, in part, guarantee:

- Proper accountability and transparency among large data holders
- Continuous independent evaluations regarding the propriety and effectiveness of data-related internal controls
- Appropriately trained internal auditors, or other qualified experts, perform risk impact assessments and other mandated evaluations to ensure objectivity.

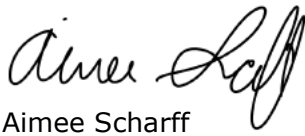
The Central Jersey and Spokane Chapters strongly endorse the proposed amendments to the ADPPA set forth by The IIA. It is our professional judgement that these recommendations will not only protect consumer data but strengthen organizational transparency and accountability.

Enclosed with this letter is a copy of The IIA's memorandum for your review and consideration. Our respective chapters would welcome an opportunity to meet with you, individually, in the coming weeks to address specific questions or concerns regarding this proposal.

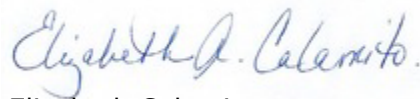
Should you have any questions regarding this request, please do not hesitate to contact Michael Downing, IIA Advocacy Director, at [Michael.Downing@TheIIA.org](mailto:Michael.Downing@TheIIA.org).

Thank you in advance for your consideration.

Respectfully,



Aimee Scharff  
President  
The Institute of Internal Auditors – Spokane  
Chapter



Elizabeth Calamito  
President  
The Institute of Internal Auditors – Central  
Jersey Chapter

Enclosure

# **PROPOSED ENHANCEMENTS TO THE AMERICAN DATA PRIVACY AND PROTECTION ACT**

## **THE INSTITUTE OF INTERNAL AUDITORS**

### **OVERVIEW OF THE ROLE OF INTERNAL AUDIT IN CORPORATIONS**

The Institute of Internal Auditors (The IIA) is the international professional association for the internal audit profession, based in Lake Mary, Florida and representing more than 230,000 internal audit professionals. The IIA is recognized as the internal audit profession's leader in standards, certification, education, research, and technical guidance.

The internal audit profession serves as the independent "eyes and ears" of an organization and internal audit functions within organizations provide objective assurance on organizational risk, corporate governance, and internal controls. In order to accomplish these objectives, an internal audit function is independent from management and reports to a governing body, a responsibility which is often delegated to the independent directors on an audit committee. This reporting relationship enables the assessments and conclusions of the internal audit function to be objective, credible, and trust-worthy.

The existence of an independent and properly resourced internal audit function enhances the value of an organization and strengthens its credibility with stakeholders. Specifically, internal audit supports a board of directors in the evaluation and understanding of:

- Effective governance, risk management, and control
- Responsible decision-making and oversight
- Sustainable value creation and protection
- Accountable stewardship of assets and reputation

The independent role of the internal audit profession is articulated in The IIA's [Three Lines Model](#) (TLM). The TLM clarifies specific corporate governance roles and responsibilities among an organization's leadership (i.e., board of directors, management, and the internal audit function) to promote strategic and operational alignment, proper oversight, and independence of the internal audit function.

It is imperative for organizations – specifically those involved in collecting and processing consumer data – to possess a clearly defined governance structure (as articulated by the TLM), including an internal audit function within the organization identifying excessive risk and potential internal control failures. Such a paradigm helps ensure sound business operations, strengthens consumer protections, and best serves the public interest.

The following document articulates a series of proposed enhancements to the American Data Privacy and Protection Act (ADPPA) intended to bolster objective assurance over corporate governance and internal controls related to data privacy and security. The IIA believes inclusion of internal audit in certain sections of the ADPPA will, in part, guarantee:

- Proper accountability and transparency among large data holders
- Continuous independent evaluations regarding the propriety and effectiveness of data-related internal controls
- Appropriately trained internal auditors, or other qualified experts, perform mandated risk impact assessments to ensure objectivity.

Should you have any questions regarding the proposal set forth by The IIA, please do not hesitate contact Michael Downing, Advocacy Director, at [Michael.Downing@TheIIA.org](mailto:Michael.Downing@TheIIA.org).

## **SUMMARY OF PROPOSED CHANGES TO THE AMERICAN DATA PRIVACY AND PROTECTION ACT**

The IIA is proposing the following changes to the American Data Privacy and Protection Act:

- Insertion of a definition for a “Certified Internal Auditor.”
- Insertion of a definition for an “internal audit function.”
- An acknowledgement by third-party collecting entities as to whether they currently have an internal audit function providing objective assurance over their internal controls.
- Clarification that the required impact assessments or evaluations on algorithms, as they relate to the civil rights provision of the bill, shall be performed by an independent researcher or other qualified expert. To the extent practicable, the covered entity’s internal audit function shall provide objective assurance to the board of directors and regulators on the effectiveness and thoroughness of the external review.
- A requirement that large data holders utilize an internal audit function to provide objective assurance over internal controls related to data security and protection of covered data.
- Clarification that certifications made by executive officers regarding internal controls and reporting structures related to data privacy and security, should be informed by objective assurance performed by the internal audit function and not by the certifying officers themselves.
- A requirement that a privacy impact assessment for large data holders conducted by the designated privacy protection officer shall be reviewed by the covered entity’s internal audit function.
- Clarification of the term “audit” as it relates to the relationship between a covered entity and a contracted service provider.

The next section provides The IIA’s proposed red-line amendments to the ADPPA. A brief commentary follows each proposed amendment to explain the rationale for the recommended modification.

## MARKED UP LEGISLATIVE LANGUAGE WITH COMMENTARY

### PROPOSAL #1:

#### Section 2. Definitions.

- Insert the following definition as Section 2(4):
  - (4) CERTIFIED INTERNAL AUDITOR.—The term “Certified Internal Auditor” means an individual who has obtained the Certified Internal Auditor credential awarded by The Institute of Internal Auditors.
- Amend the subsequent numbered bullets in Section 2 to reflect the insertion of the Certified Internal Auditor definition in paragraph (4).

**COMMENT:** This proposed subsection defines the term “Certified Internal Auditor” which is now referenced in Section 2(18).

The Certified Internal Auditor (CIA) credential is the only globally recognized certification for the practice of internal audit. The professional credential is awarded by the Institute of Internal Auditors following completion of a rigorous exam and work experience requirements. CIA’s must also complete an annual continuing education program to maintain an active certification.

The CIA designation sets the standard for excellence within the profession and reflects the highest level of internal audit expertise. Over 170,000 CIAs have been issued globally since the credential was first launched.

More information regarding the Certified Internal Auditor credential can be accessed at <https://www.theiia.org/en/certifications/cia/>.

### PROPOSAL #2:

#### Section 2. Definitions.

- Insert the following definition as Section 2(18):
  - (18) 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 with strategic advice on risk mitigation. For the purposes of this Act, 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 data privacy and security.
- (ii) No provision in this Act 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.

- Amend the subsequent numbered bullets in Section 2 to reflect the insertion of the “internal audit function” definition in paragraph (18).

**COMMENT:** This subsection defines the term “internal audit function” and establishes minimum criteria for the internal audit function to ensure it:

- Conforms with corporate governance best practices, such as the updated [Three Lines Model](#)
- Effectively provides objective assurance over the covered entity’s internal controls.

For purposes of this Act, the definition places a special emphasis on guaranteeing expertise among internal audit staff as it relates to data privacy and security.

The definition also retains maximum flexibility in the structure of organizational internal audit functions. For example, while most internal audit functions are truly internal, some corporations, on occasion, will contract out some or all of their internal audit function. Nothing in this Act would preclude outsourcing or co-sourcing the internal audit function provided it does not create a conflict of interest in the provision of external audit services.

**PROPOSAL #3:**

SECTION 206. THIRD-PARTY COLLECTING ENTITIES.

- Insert the following language as Section 206(b)(2)(B)(iii):
  - (iii) Acknowledgement of whether the third-party collecting entity possesses an internal audit function to provide objective assurance over the covered entity’s internal controls over data privacy and security processes and procedures.
- Amend the subsequent numbered bullets in Section 206(b)(2)(B) to reflect the insertion of subparagraph (iii).

**COMMENT:** Section 206 pertains to the obligations of third-party collecting entities. Under the Act, third-party collecting entities must, in certain circumstances, post a public notice online that they are a third-party collecting entity and are required to register with the Federal Trade Commission (Commission) or face financial penalties. In their registration, third-party collecting entities must

share specific information, including their legal name and address, a description of the categories of data they process and transfer, contact information, and a link to a website where an individual may exercise his or her rights. This information will then be shared on a publicly searchable Commission website and individuals will have the right on the site to have their data deleted by the covered entity and an affirmative express consent requirement imposed on the collection of future data.

The newly proposed language above would add information to the Commission registry about whether the third-party collecting entity has an internal audit function which provides objective assurance over the entity's internal controls. Such an acknowledgment would provide valuable information about the consumer protection safeguards at the third-party collecting entity without mandating an internal audit function. The public could then make a more informed choice about the level of confidence they may have in such an entity.

Meanwhile, in a free market, third-party collecting entities, which may vary in size and resources, can perform a cost-benefit assessment whether to invest in an internal audit function providing objective assurance over data privacy and security internal controls based on perceived public demand.

#### **PROPOSAL #4:**

##### SECTION 207. CIVIL RIGHTS AND ALGORITHMS.

- Amend Section 207(c)(3)(B) as follows:
  - (B) EXTERNAL, INDEPENDENT ~~AUDITOR OR~~ RESEARCHER OR OTHER QUALIFIED EXPERT.—To the extent possible, a covered entity and a service provider shall utilize an external, independent ~~auditor or~~ researcher, or other qualified expert, to conduct an impact assessment under paragraph (1) or an evaluation under paragraph (2).
    - (i) The independent impact assessment or evaluation performed under paragraph (B) shall, to the extent possible, be reviewed by the covered entity's internal audit function to provide the board of directors and regulators with objective assurance regarding the effectiveness and thoroughness of the impact assessment.

**COMMENT:** Section 207(c) establishes a requirement that large data holders conduct an annual algorithm impact assessment – beginning two years after enactment of the legislation – to ensure the mode of data collection does not “cause potential harm to an individual.” The amendment to Section 207(c)(3)(B) clarifies that an “independent researcher, or other qualified expert,” shall be responsible for leading the internal impact assessment or evaluation set forth in paragraphs (1) and (2). Since an impact assessment is not an audit – either external or internal – eliminating the term “auditor” more accurately represents the type of work being performed.

The proposal also includes the insertion of subparagraph (i) creating a new requirement that the impact assessment performed under Section 207(c) shall be reviewed, to the extent practicable, by the covered entity's internal audit function. The internal audit function of an organization is responsible for providing objective assurance, independent from management, on subjects related to risk and internal controls. Internal auditors are trained to continuously evaluate the systems and actions of an organization to ensure potential consumer risks are identified and mitigated.

Therefore, requiring the internal audit function to review the impact assessment mandated by Section 207(c) provides the board of directors with objective assurance on the effectiveness and thoroughness of the evaluation; strengthens organizational accountability; and promotes consumer protection.

**PROPOSAL #5:**

SECTION 208. DATA SECURITY AND PROTECTION OF COVERED DATA.

- Insert the following language as Section 208(b)(8):
  - (8) OBJECTIVE ASSURANCE OVER INTERNAL CONTROLS.— For large data holders, the covered entity’s internal audit function shall provide, on an on-going basis, objective assurance over the entity’s internal controls related to data security and privacy practices and report its findings, not less than once a year to: executive management; the full board of directors and/or a designated committee of the board comprised exclusively of independent directors.

**COMMENT:** Section 208 requires a covered entity or service provider to “establish, implement, and maintain reasonable administrative, technical, and physical data security practices and procedures to protect and secure covered data against unauthorized access and acquisition.” It identifies specific considerations in developing the practices and procedures and enumerates requirements that all covered entities’ data security practices must contain.

Section (208)(b)(8) would add an additional requirement for large data holders: to use their internal audit function to provide objective assurance over internal controls related to these data security and privacy practices.

Such a safeguard is an ***essential*** provision to ensure that these large data holders are effectively protecting their customers. It would be poor corporate governance and violate the spirit of this Act to establish these consumer protections and then never test and report on their effectiveness. Indeed, failure to provide assurance over these large data holders’ internal controls greatly increases the likelihood of data breaches, ransomware attacks, corporate theft, and exposure of customers’ personal information.

Unlike the proposed language of Section 206(b)(2)(B)(iii) seeking disclosure as to whether a third-party collecting entity has an internal audit function, this language mandates that a large data holder utilize its internal audit function to provide assurance over data privacy and security internal controls and then report on its findings. These covered entities are of a large enough size and the risk to the public is so great, that this type of safeguard should not be optional.

How else will large data holders know that their data privacy and security practices are effective, safe, and properly operating without assurance over their internal controls? In short, these organizations will not have the requisite information to verify such claims without an appropriate internal audit.

Indeed, The IIA believes that failure by large data holders to internally test and report on their data privacy internal controls would undermine the entire consumer protection goals of this Act.

**PROPOSAL #6:**

SECTION 301. EXECUTIVE RESPONSIBILITY.



- Amend Section 301(b) as follows:
  - (b) REQUIREMENTS.—A certification submitted under subsection (a) shall be based on a review of the effectiveness of a large data holder’s internal controls and reporting structures that is conducted by the ~~certifying officers~~ covered entity’s internal audit function not more than 90 days before the submission of the certification.

**COMMENT:** Section 301 establishes a process for executive officers of large data holders to certify, annually, that the covered entity possesses “internal controls reasonably designed to comply with this Act.” The current language, however, requires the certifying officer to conduct a review of the effectiveness of internal controls and reporting structures not more than 90 days before submission of the certification.

The proposed amendment to Section 301(b) empowers the covered entity’s internal audit function – not the certifying official – with conducting the mandated review of internal controls and reporting structures. Since internal auditors operate independent from management, these professionals are best equipped to objectively evaluate the appropriateness and effectiveness of internal controls related to data privacy and security.

**PROPOSAL #7:**

SECTION 301. EXECUTIVE RESPONSIBILITY.

- Insert the following language as Section 301(d)(2)(C)(i):
  - (i) The privacy impact assessment performed under paragraph (B) shall be reviewed by the covered entity’s internal audit function to provide the board of directors and regulators with objective assurance regarding the effectiveness and thoroughness of the evaluation.

**COMMENT:** Section 301(d)(1) establishes a requirement that large data holders must, biennially, conduct a privacy impact assessment to measure the benefits and risks of organizational data collection practices on individual privacy.

The proposed insertion of subparagraph (i) to Section 301(d)(2)(C) requires that the privacy impact assessment should be reviewed by the covered entity’s internal audit function to provide the board of directors with objective assurance that the evaluation was effective and thorough.

**PROPOSAL #8:**

SECTION 302. SERVICE PROVIDERS AND THIRD PARTIES.

- Amend Section 302(b)(4)(B) as follows:
  - (B) combining service provider data with covered data which the service provider receives from or on behalf of another person or persons or collects from its own interaction with an individual. The contract may, subject to agreement with the service provider, permit a covered entity to monitor the service provider’s compliance with the contract through measures including, but not limited to, ongoing manual reviews and

automated scans, and regular assessments, second- or third-party audits, or other technical and operational testing at least once every 12 months.

**COMMENT:** The technical amendment to Section 302(b)(4)(B) clarifies the type of audits a covered entity may perform, subject to the contractual agreement, with a service provider in accordance with the Act.

A second-party audit permits the covered entity (or a contracted external auditor) to evaluate the service providers' compliance with the contract terms and conditions. Although a third-party audit assesses the same information as a second-party audit, it is conducted by an independent external auditor to guarantee objectivity.