

# AIF Coalition for the Future of Artificial Intelligence (AI) in Business



## Executive Summary



ASSOCIATED INDUSTRIES OF FLORIDA  
*The Voice of Florida Business Since 1920*

# AIF Coalition for the Future of AI in Business

## Coalition Mission

Bring business sectors together to: (1) develop guidelines for accountable and innovative AI policies and

(2) educate and engage with policymakers to ensure a responsible regulatory structure.

## Coalition Activities

### Educational Component

- Familiarize key legislative leaders with how AI is currently being implemented in the business community in a broad way and discuss future applications.
- Hold round table events to bring legislative leaders and business leaders together to discuss the issue and its future impact.

### Policy Component

- Develop and pass a broadly agreed upon definition of AI to be used as a launching point for policy development in the future.

## Coalition Membership

Using the unmatched expertise of AIF members in collaboration with non-AIF members and stakeholders with AI expertise, the Coalition will be comprised of the following levels:

### Founding Members

These AIF members will be instrumental in establishing policy guidelines and have final approval of the Coalition's work product.

### Workgroup Leaders

Several workgroups will be formed to do the preliminary work on the various sectors of AI that need to be explored.

### Partner Members

Non-AIF organizations that provide expertise and critical input and participate with the workgroups.



Sen. Joe Gruters (R), Rep. Christine Hunschofsky (D) listen to concerns from business leaders at the Foundation of Associated Industries of Florida AI round table.



*There is strong consensus among elected officials and business leaders in the United States that thoughtful measures are necessary to prevent bad actors from using AI to impose harm to others or threaten our national security. As we consider proposals for legislation or regulation, it is critically important that policies continue to foster innovation and promote the adaptation of emerging technologies.*

– BREWSTER B. BEVIS, PRESIDENT & CEO, AIF



## Overview

Artificial intelligence (AI) is a transformative technology with limitless applications for manufacturing, transportation, health care, agriculture, defense, and many other areas.

Although Congress has not approved new AI laws, there appears to be a consensus among elected officials and business leaders that thoughtful measures are necessary to prevent bad actors from using AI to harm others or threaten national security. However, legislation and subsequent regulatory guidelines must foster innovation and promote the adaptation of emerging technologies.

A piecemeal approach to state regulation of AI can lead to a fragmented regulatory landscape that may exacerbate existing issues and create new challenges. When individual states implement their own regulations, the lack of uniformity can lead to confusion and inefficiency for businesses that operate across state lines, potentially stifling innovation and increasing compliance costs. Additionally, such an approach may result in regulatory gaps where certain risks are inadequately addressed, as different states may focus on disparate aspects of AI, such as privacy, safety, or ethical considerations. This inconsistency can undermine efforts to establish comprehensive safeguards and may inadvertently encourage companies to relocate or adjust their practices to the most lenient jurisdictions, diminishing the overall effectiveness of regulatory measures and potentially exacerbating the risks associated with AI technology.



## Florida Action

The 2024 Florida Legislature considered several proposals to define and address the use of artificial intelligence. Outlined below are the proposals and their final result:

AI in Political Advertisements | HB 919 prescribed new regulations on AI use in political advertisements and defined “generative artificial intelligence.” The Legislature approved HB 919, which was signed into law by Governor DeSantis. The legislation took effect July 1, 2024.

**Advanced Technology (Senate) | SB 1680** created the Government Technology Modernization Council to assess the impact of automated decision systems and identity management on Florida residents’ constitutional and legal rights. The Council will evaluate AI safety and security standards, such as requiring digital provenance disclosure for generative AI creations. The council will also assess AI usage by governmental and private sectors for statewide deployment opportunities, investigate AI exploitation by malicious entities, and determine the need for digital media and visual literacy curricula for school-age audiences. The Legislature approved SB 1680, which was signed into law by Governor DeSantis. The legislation took effect July 1, 2024.

## Advanced Technology (House) | CS/CS/HB 1459

was the companion bill to SB 100, which was ultimately approved. The proposed House version contained provisions that differed from what ultimately was approved in SB 100. In this summary, “proposed language” refers to language proposed in HB 1459.

## The Role of the AIF Coalition

As an advocate for Florida businesses for over 100 years, AIF understands the need to engage with policymakers on emerging issues before public policy measures are approved.

The Coalition has brought together key legislative leaders with leading AI representatives from many business sectors to help reach a common goal: Ensure Florida AI laws and regulations provide a reasonable structure by which the interest and safety of the public are protected while allowing innovation to continue.

### How Current Florida Statutes Address AI

Before the Legislature proposes comprehensive AI legislation, evaluating how current state statutes regulate the issue is imperative. In particular, many statutes that are silent on AI may preclude certain actions whether they are achieved through the use of AI or another mechanism. Without this evaluation, the Legislature could develop and improve duplicative and unnecessary regulation. Further, a thorough review will determine if current statutes limit the appropriate use of AI and if modernization of statutes is needed.

For example, Florida’s data privacy laws may enhance or conflict with proposed AI legislation, given the use of data in training and executing AI models. Future proposed legislation should define objective tests that can be applied to operational use cases regardless of whether AI enables the use cases.

Absent a full understanding of how Florida’s laws and rules already impact AI development, deployment, and use, companies may be slow to innovate in order to avoid negligence or discrimination claims. For example, a well-intentioned AI system may include biases not noticed during testing that could result in legal claims for civil rights violations.

## Florida Government Technology Modernization Council

This Council, created during the 2024 Legislative Session, is the appropriate body to conduct the comprehensive evaluation with solicited input from business stakeholders. The Council’s first report is due to the Governor and the Legislature on December 31, 2024. An annual report is due each December 31 after that and must provide recommendations to:

- Increase productivity of state enterprise information technology systems;
- Improve customer service levels of government and reduce administrative or operating costs;
- Promote development/deployment of AI systems, financial technology, education technology, or other enterprise management software; and,
- Protect Floridians from bad actors who use AI.

At the time of publication, the following members are appointed to the Council:

- Lt. Governor Nunez, serving as Chair
- State Chief Information Officer
- Secretary of Commerce (or designee)
- Secretary of AHCA (or designee)
- Secretary of Transportation (or designee)
- Executive Director of FDLE (or designee)
- Five from the industry appointed by various officials
  - Governor Appointee:
  - Governor Appointee:
  - Governor Appointee:
  - Senate: Jonathan Fozard, CIO, Florida State University
  - House: John Damalas, Group Vice President and Chief Technology Officer, JM Family Enterprises
- Senator Jason Brodeur (Senate appointee)
- Representative Fiona McFarland (House appointee)





# Analysis and Recommendations from the AI Coalition

This executive summary discusses the following components of AI policy: Definitions, Transparency, and Enforcement. Each section of the report will:

- Provide the status of language approved previously proposed in Florida;
- Summarize concerns associated with the approved or proposed language; and,
- Provide recommendations for policymakers' consideration.

## Definitions

**Florida House Bill 919** defines "generative artificial intelligence" as:

*106.145 Use of artificial intelligence.  
(1) As used in this section, the term "generative artificial intelligence" means a machine-based system that can, for a given set of human-defined objectives, emulate the structure and characteristics of input data in order to generate derived synthetic content, including images, videos, audio, text, and other digital content.*

## Concerns and Recommendations

The definition contained in HB 919 combines an AI definition with a specific type of AI, limiting flexibility for future legislation and interoperability with other states.

**Recommendation #1:** Continue to monitor the work of the U.S. Department of Commerce National Institute for Standards and Technology (NIST).

**Recommendation #2:** Consider the following principles when defining AI and generative AI:

- Limit definitions to system that make decisions and impact the public.
- Ensure definitions are clear and concise to align with the areas of perceived risk and avoid interpretation outside the intended context
- Align definitions with others approved to provide regulatory certainty for businesses across the United States and avoid confusion about consumer rights.

## Transparency

One of the biggest challenges and opportunities with the language proposed in HB 1459 was ensuring the language was clear and concise to avoid costs associated with varying interpretations. This is especially important given the lack of industry-wide or federally-mandated standards.

HB 1459 sought to establish an AI-related transparency process for businesses. This proposed language stated:

*The "entity or person who produces or offers for use or interaction artificial intelligence content or technology for a commercial purpose, and makes such content or technology available to the Florida public, must create safety and transparency standards that:*

- (a) Alert consumers that such content or technology is generated by artificial intelligence;*
- (b) Allow such content or technology to be recognizable as generated by artificial intelligence to other artificial intelligence.*

*If a natural person in this state is able to communicate or interact with an entity or person for commercial purposes through an artificial intelligence mechanism, such entity or person must provide a clear and conspicuous statement on the entity's or person's Internet homepage or landing page that such mechanism is generated by artificial intelligence.*

*An entity or person may not knowingly produce, generate, incorporate, or synthesize through artificial intelligence child pornography as defined in s. 775.0847(1).*

*Any state agency as defined in s. 282.318(2) which uses artificial intelligence must disclose if a person is interacting with artificial intelligence when interacting with the agency and ensure that any confidential information accessible to an artificial intelligence system remains confidential.*

## Concerns and Recommendations

**High-Risk Versus Low-Risk AI Uses:** High-risk AI systems, such as those used in healthcare, autonomous vehicles, or critical infrastructure, pose significant ethical, safety, and privacy concerns that necessitate stringent oversight to protect citizens and maintain public trust. In contrast, low-risk applications like chatbots or basic data analysis tools may warrant more flexible regulations to encourage entrepreneurship and technological advancement.

Tailoring regulations to the specific risk profiles of AI applications can ensure a balanced environment in Florida that promotes responsible innovation while safeguarding the welfare of its residents. This nuanced approach can help prevent stifling technological growth while ensuring that AI's benefits are realized safely and ethically.

**Recommendation:** Consider the distinction between high-risk and low-risk applications of AI when developing a regulatory framework that can enhance innovation and safety.

**Regulatory Scope:** The term "available to the Florida public" is very broad and appears to regulate anyone with a website, even companies with no intention of reaching Florida residents. This language could have constitutional concerns.

**Recommendation:**

- Limit regulation to high-risk uses of AI that directly make consequential significant decisions about consumers and video/images that will materially mislead consumers about actual events.
- Consider clarifying the intent of any proposed legislation to reach companies doing business in Florida or engaging Florida residents.

**Standards & Disclosure:** The requirement in the proposed legislation that a company "create safety and transparency standards" and that those standards "alert consumers" and "allow such content" to be recognized as AI-generated is unclear. The proposed language, which states "offers for use or interaction," could be interpreted to include the presence of text or images on a website.

**Recommendation:** Consider clarifying the terms "use" or "interact." For example, does static web content count as an "interaction" because the consumer visits a webpage and reads or views the content?

The obligation to disclose interaction with an AI system does not appear to be tied to the actual place of the interaction. For example, the homepage of a company's site may disclose AI usage; however, the actual usage of AI may be on pages deeper on the site. A user may not recall the homepage warning, or if they skip the homepage, they may not view the warning at all.

**Recommendation:** Consider requiring the disclosure to be made on the page where the user will interact with the high-risk AI system.

The NIST Cybersecurity Framework (CSF) contains provisions for a voluntary certification program for businesses to subject themselves to a well-structured external review in exchange for credentials that increase credibility and trust with the public and policymakers.

**Recommendation:** Consider establishing a voluntary certification framework mirroring the NIST CSF. Participation in NIST's multi-stakeholder processes is encouraged to ensure all stakeholders' concerns are addressed.

Companies often use generative AI as a starting point for drafting content or creating images, but then they revise the content. Requiring disclosure for all content will stifle efficiency-generating tools, lead to over-notification, desensitize the user, and reduce the usefulness of the notice.

**Recommendation:** Consider limiting the required disclosures of high-risk AI to situations where a human has not materially altered the output.

Requiring companies to enable every AI to detect whether the content is AI-generated is impractical, as some systems do not have that capability or purpose. The requirement could result in a company being deemed non-compliant, even if there is no need for the system to have that capability.

**Recommendation:**

- Consider not requiring companies to make generative AI content recognizable by other forms of AI.
- Consider allowing the Department of Legal Affairs to issue rules specifying the standards sufficient for compliance.

**Enforcement**

Appropriate enforcement measures must focus on two components:

- Incentivizing businesses to “do the right thing” by proactively building safeguards and taking action when vulnerabilities are identified; and
- Penalizing businesses that fail to act appropriately when vulnerabilities or risks are identified.

**CS/CS/HB 1459 Advanced Technology**

proposed the following language:

*(6)(a) Any violation of subsection (2), subsection (3), or subsection (4) is an unfair and deceptive trade practice actionable under part II of chapter 501 solely by the department. If the department has reason to believe that a violation of this section has occurred, the department, as the enforcing authority, may bring an action for an unfair or deceptive act or practice. For the purpose of bringing an action pursuant to this section, ss. 501.211 and 501.212 do not apply. In addition to other remedies under part II of chapter 501, the department may collect a civil penalty of up to \$50,000 per violation of this section.*



Chris Hein of Google provided valuable input on the AI issue.

*(b) This section does not establish a private cause of action.*

*(7) For purposes of bringing an action pursuant to this section, any entity or person who produces or uses artificial intelligence that is distributed to or viewable by the public in this state is considered to be both engaged in substantial and not isolated activities within this state and operating, conducting, engaging in, or carrying on a business, and doing business in this state, and is therefore subject to the jurisdiction of the courts of this state.*

### **Concerns and Recommendations:**

#### **Rebuttable Presumption & Affirmative Defense:**

These concepts are imperative to promoting responsible innovation while safeguarding the welfare of its residents:

*Rebuttable presumption* should be extended to developers and deployers who have used reasonable care and adhered to specific requirements, including implementing a risk management policy and program closely aligned with the latest version of the NIST AI RMF or another nationally- or internationally-recognized risk management framework.

*Affirmative defense* should be permitted for developers and deployers if they discover and correct a violation through internal testing or “red teaming” and comply with the NIST AI RMF or other recognized risk management framework.

**Recommendation:** Consider including rebuttable presumption and affirmative defense language provisions in future proposed legislation.

**Right to Cure:** The proposed language in HB 1459 did not allow the opportunity to correct an issue before being fined or sued.

The Colorado AI Act provides an affirmative defense to a company that discovers and corrects a violation after receiving notice from a third party, discovering the issue due to adversarial testing, or conducting an internal review so long as the company also complies with the applicable NIST framework (or an approved alternative). Further, a version of language proposed in Connecticut (SB 2) included traditional “right to cure” provisions.

**Recommendation:** Consider providing a “right to cure” provision on issues related to alerting consumers to generative AI content, making content recognizable to AI, and requiring notice if a user interacts with AI.

**Violation Standard & Accrual:** It is important to insert a “knowingly” standard for a violation to occur to ensure a business cannot be fined or sued if the error is unknown. Recommendation: Add the following language: “(7) For purposes of bringing an action pursuant to this section, any entity or person who knowingly produces...”

The language proposed in HB 1459 is vague on what constitutes a violation allowing for varying interpretation, such as:

- A violation accrues for each visitor, and each time they visit the webpage or
- A violation accrues for each visitor upon their first visit to the webpage or
- A violation accrues once regardless of the number of people affected or the number of visits to the webpage.



The proposed language in HB 1459 was unclear as to when a violation occurs. Other states' similar legislative vagueness has confusion, litigation and potentially tremendous costs for businesses. For example, the Illinois Biometric Information Privacy Act (BIPA), contained vague violation language. Ultimately, the Illinois Supreme Court held that a claim accrued for each scan for each person, leading to potential astronomical damages. The 2024 Illinois legislature subsequently clarified that claims accrue for the first violation for each person only.

**Recommendation:** Consider clarifying what constitutes a violation and when a violation occurs in future proposals addressing violations related to alerting consumers to generative AI content, making the content recognizable to AI, and requiring notice of interacting with AI.

**Penalties:** Any language on penalties must be clear and transparent to ensure businesses understand the consequences of their actions, and any penalty should be assessed uniformly.

Further, the accrual period should be clear, and punishment must be proportionate to the offense. The language proposed in HB 1459 did not provide guidance on how the penalty would be calculated.

**Recommendation:** Consider adding criteria for calculating a penalty, such as intentional or repeated violations, attempted remediation, or self-reporting. For consideration is the Maryland privacy law § 14-4613(D), which determines when to grant a right to cure. It states:

In determining whether to grant a controller or processor an opportunity to cure an alleged violation, the division may consider the following factors:

- (1) *the number of violations;*
- (2) *the size and complexity of the controller or processor;*
- (3) *the nature and extent of the controller's or processor's processing activities;*
- (4) *the likelihood of injury to the public;*

- (5) *the safety of persons or property;*
- (6) *whether the alleged violation was likely caused by a human or technical error; and*
- (7) *the extent to which the controller or processor has violated this subtitle or similar laws in the past.*

Finally, the language in HB 1459 proposed an unusually high maximum penalty of \$50,000 per violation. Current Florida privacy law violations levy \$7,500 per violation. The Utah generative AI legislation limits penalties to \$2,500 per violation.

**Recommendation:** Consider lowering and capping the maximum penalty for violations.

**Private Right of Action:** Placing a private cause of action in future legislation will stifle innovation in Florida. The result can be frivolous lawsuits filed by plaintiff's attorneys seeking a "deep pocket" that significantly drains a company's resources, which would be used for compliance improvements.

**Recommendation:** Future proposals should include the following statement: "Nothing in this chapter shall be construed as providing the basis for a private right of action for violations of said provisions."



For more information on the Coalition, please contact  
**Adam Basford, Vice-President of  
Governmental Affairs (abasford@aif.com).**



# Resources

## 1. **U.S. Department of Commerce National Institute for Standards and Technology (NIST) –**

The following statement can be found at: <https://www.nist.gov/artificial-intelligence>:  
“NIST aims to cultivate trust in the design, development, use and governance of Artificial Intelligence (AI) technologies and systems in ways that enhance safety and security and improve quality of life. NIST focuses on improving measurement science, technology, standards, and related tools — including evaluation and data.

With AI and Machine Learning (ML) changing how society addresses challenges and opportunities, the trustworthiness of AI technologies is critical. Trustworthy AI systems are those demonstrated to be valid and reliable; safe, secure, and resilient; accountable and transparent; explainable and interpretable; privacy-enhanced; and fair with harmful bias managed. The agency’s AI goals and activities are driven by its statutory mandates, Presidential Executive Orders and policies, and the needs expressed by U.S. industry, the global research community, other federal agencies, and civil society.

The NIST-AI-600-1, Artificial Intelligence Risk Management Framework: Generative AI Profile (AI RMF), assists organizations in deciding how to best manage AI risks in a manner that is aligned with their goals. It also considers legal and regulatory requirements and best practices, reflecting risk management priorities. The profile offers insights into how risk can be managed across various stages of the AI lifecycle and for GAI as a technology. The AI RMF and the corresponding NIST AI RMF Playbook suggest organizations voluntarily define and develop certification procedures for operating AI systems within defined contexts of use.

## 1. **Coalition for Content Provenance and Authenticity (C2PA) – The following information can be found at:** <https://c2pa.org/>

The Coalition for Content Provenance and Authenticity (C2PA) is a project of the Joint Development Foundation, a Washington-based 501c6 non-profit, that brings together the efforts of the Content Authenticity Initiative (CAI) and Project Origin.

Founded in late 2019 by Adobe in collaboration with the New York Times and Twitter, the CAI is building a system to provide provenance and history for digital media, providing a tool for creators to claim authorship while empowering consumers to make informed decisions about what to trust. Project Origin, founded in 2019 by BBC, CBC Radio Canada, Microsoft, and the New York Times, focuses on tackling disinformation in digital news by defining an end-to-end process for publishing, distribution, and attaching signals to e-content to demonstrate its integrity.

The C2PA binds the efforts of these two groups and focuses exclusively on the development of open, global technical standards to channel the content provenance efforts of the CAI and Project Origin. C2PA is tasked with:

- Documenting workflow requirements as informed by CAI, Project Origin, and other partner organizations
- Applying those requirements in development of content provenance specifications
- Developing best practices and reference designs for applying those standards
- Promoting selected specifications to become global standards
- Promoting global adoption of digital provenance techniques
- Promoting adoption of digital Coalition’s specifications and standards by social and media platforms
- Ensuring content remains accessible even with digital provenance techniques applied

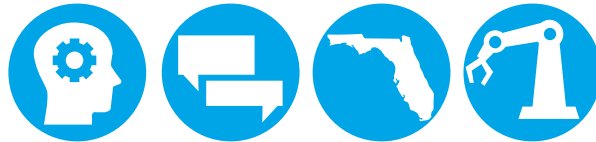
The Coalition for Content Provenance and Authenticity (C2PA) established technical standards for certifying the source and history (or provenance) of media content. Although detection and determination of content as artificial intelligence-generated content (AIGC) will always be impractical, the C2PA standards approach the issue differently and allow creators to assert through provenance the authenticity of content. The site contains the various specifications and documents produced by the C2PA, including:

- Technical Specifications
- Explainer
- Guidance for Implementers
- User Experience Guidance
- Security Considerations
- Harms Modelling



**AIF Coalition for the Future of  
Artificial Intelligence (AI)**

**in Business**



**Associated Industries of Florida**




 516 North Adams Street • Tallahassee, Florida 32301

 850.224.7173

 aif@aif.com

 **AIF.com**

 @VoiceofFLBiz