LFC Requester:	Chavez

AGENCY BILL ANALYSIS - 2025 REGULAR SESSION

WITHIN 24 HOURS OF BILL POSTING, UPLOAD ANALYSIS TO
AgencyAnalysis.nmlegis.gov and email to billanalysis@dfa.nm.gov
(Analysis must be uploaded as a PDF)

SECTION I: GENERAL INFORMATION
{Indicate if analysis is on an original bill, amendment, substitute or a correction of a previous bill}

Date Prepared: 2/13/25   *Check all that apply:*

Bill Number: HB 401   Original   x____   Correction   ____

Amendment   ____   Substitute   ____

Sponsor: Rep. Serrato

Agency Name and Code Number: NM DoIT - 361

Person Writing Analysis: Jason L. Clack

Short Title: A.I. Synthetic Content Accountability Act

Phone: 505-500-9291   **Email:** Jason.clack@doit.nm.gov

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY25	**FY26**		
0	0		

(Parenthesis ( ) indicate expenditure decreases)

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY25	**FY26**	**FY27**		
0	0	0		

(Parenthesis ( ) indicate revenue decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY25	FY26	FY27	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total						

Duplicates/Conflicts with/Companion to/Relates to:
Duplicates/Relates to Appropriation in the General Appropriation Act

SECTION III: NARRATIVE

BILL SUMMARY

Synopsis: House Bill 401 (HB 401) would create the Artificial Intelligence Synthetic Content Accountability Act (the Act).

The Act would contain definitions for the terms "artificial intelligence," "artificial intelligence red-teaming," "biometric system," "content," "covered synthetic content," "depicted person," "digital fingerprint," "digital identification," "digital signature," "generative artificial intelligence system," "large online platform," "minor modification," "nonsynthetic content," "provenance data," "provider," "reasonable identity verification method," "state-of-the-art techniques," "synthetic content," "transactional data," "watermark," and "watermark decoder".

The Act would create a private cause of action against a person for the nonconsensual dissemination of covered synthetic content, which includes "content that has been produced or significantly modified from its original form by a generative artificial intelligence system" other than text. This cause of action would exist when someone publicly disseminates covered synthetic content with: (a) knowledge that a depicted person in the covered synthetic content did not consent to the dissemination; and (b) the intent to harass, entrap, defame, extort or otherwise cause financial or reputational harm to the depicted person. The content would also have to realistically represent a depicted person engaging in conduct that the depicted person did not actually engage in, and the depicted person is identifiable from: (a) the covered synthetic content alone; or (b) other personal information displayed or disseminated in connection with the covered synthetic content. There would be exceptions if:

1. The dissemination is made: (a) for the purpose of a criminal investigation or prosecution that is otherwise lawful; (b) for the purpose of or in connection with a report of unlawful conduct to appropriate authorities; or (c) in the course of seeking or receiving medical or mental health treatment, and the covered synthetic content is protected from further dissemination by the recipient.
2. The person who disseminated the covered synthetic content commercially obtained the content for the purpose of the person's lawful sale of goods or services, including artistic creations, and the depicted person knew that the covered synthetic content would be created and disseminated commercially.
3. The covered synthetic content relates to a matter of public interest; the dissemination of the content serves a lawful public purpose; and the person that disseminates the content clearly identifies that the content is covered synthetic content.
4. The dissemination is for legitimate scientific research or educational purposes, the covered synthetic content is clearly identified as such and the person who disseminates the content acts in good faith to minimize the risk that the covered synthetic content will be further disseminated.
5. The dissemination is made for use in legal proceedings and: (a) is consistent with common practice in civil proceedings necessary for the proper functioning of the court system; or (b) the content is protected by court order that prohibits any further dissemination.

6. The dissemination constitutes criticism, comment, satire, parody, news reporting, teaching, scholarship or research and a reasonable consumer receiving the content would not believe it to accurately represent the depicted person's speech or conduct.

The court would be allowed to issue orders to protect the privacy of the plaintiff in these actions. A prevailing plaintiff would be allowed to recover attorney's fees, liquidated damages of $10,000, or actual damages.

The Act would also create criminal liability if improper dissemination of covered synthetic content consists of knowingly disseminating or presenting any likeness of an identifiable person in covered synthetic content with the purpose of harassing, entrapping, defaming, extorting or otherwise causing financial or reputational harm to the depicted person. A person found criminally liable would be guilty of a fourth-degree felony.

The Act would require a provider to place an imperceptible watermark that is designed to be as difficult to remove as is reasonably possible using state-of-the-art techniques into covered synthetic content that is produced or significantly modified by a generative artificial intelligence system that the provider makes available. If the content is too small to watermark, the provider would have to, at a minimum, attempt to embed provenance data into the content that identifies the content as partially or entirely synthetic, with other required information about the provider and content. The provider would also have to make a watermark decoder available at no cost. Providers would also be required to conduct artificial intelligence red-teaming involving third-party experts to test whether watermarks in the system can be easily removed from covered synthetic content, or if the provider's generative artificial intelligence systems can be used to falsely add watermarks to otherwise nonsynthetic content. Also, if the system can be downloaded and modified, the provider would have to conduct red-teaming to assess whether the system's watermark functionalities can be disabled without authorization. A provider would have to make summaries of its artificial intelligence red-teaming exercises publicly available in electronic form and submit a full report of each artificial intelligence red-teaming exercise it conducts to the attorney general within six months of completion. Developers would have to report to the attorney general within ninety-six hours of discovering a material vulnerability or failure in a generative artificial intelligence system related to the erroneous or malicious inclusion or removal of provenance data or watermarks. They would also have to notify other developers and other parties affected by the vulnerability or failure. Any report to the attorney general would also have to be made publicly available. Large online platforms would be required to use the provenance data of content and state-of-the-art techniques to classify and label content that is uploaded by users. Users would have a reasonable opportunity to appeal the classification of content by a large online platform.

The attorney general would have enforcement authority over the provisions of the Act.

The Act would require a large online platform to use a reasonable identity verification method to verify a platform user's identity before allowing the user to post content on the platform if the content (1) was classified by the platform as fully synthetic, partially synthetic or possibly covered synthetic content of unknown provenance; and (2) purports to depict reality. The platform would be required to protect any information obtained while performing these actions. They would not be able to use this identification information for any other purpose and would only be able to disclose this information pursuant to court order.

FISCAL IMPLICATIONS

As explained further below, the watermarking, red-teaming, and reporting requirements of the Act, will increase the cost of AI contracting for state agencies. Because state agencies will not be engaging in the type of conduct that the Act seeks to guard against, these costs could be saved if the agencies are exempt from those requirements. This is new technology and new processes which the Act is asking for AI vendors to develop, and therefore the costs associated with these requirements is currently unknown, and unquantifiable with regard to the types of AI services that the state would be looking to procure. However, as these costs would be part of the scope of work for any generative AI project, other than text, then they would increase the cost of those contracts for the state commensurate to the cost of compliance by the vendor.

SIGNIFICANT ISSUES

Under the Act, a "provider" means an individual who or an entity that creates, codes, substantially modifies or otherwise produces a generative artificial intelligence system. The Act creates protections for covered synthetic content that depicts individuals and is distributed for prohibited purposes. State agencies would not be impacted by these protections, because agencies would not be using AI for those purposes. However, the Act would require providers to place watermarks on all "covered synthetic content" which is "content that has been produced or significantly modified from its original form by a generative artificial intelligence system" other than text. Vendors that develop AI systems for state agencies for purposes of increasing work productivity and improving performance could be considered as "developers" under the Act. Therefore, any AI content that is generated by the agencies' generative AI systems, other than text, would be required to follow this watermarking requirement, even if that content does not depict any individuals or is not distributed for any improper purposes. The agencies would also be required to conduct the artificial intelligence red-teaming, involving third-party experts, before the release of any new generative artificial intelligence system. Agencies would also be required to comply with the reporting requirements associated with the red-teaming.

These requirements would greatly increase the cost of contracting for the development and implementation of AI systems by state agencies. State agencies would have to make these contractual requirements for the vendors, in order to comply with the Act. This would greatly increase the cost of these contracts and potentially reduce the availability of AI vendors in the state. The requirements would also create a competitive disadvantage for smaller AI vendors which may not have the resources to meet these requirements. This approach would greatly stifle the ability of state agencies to procure AI systems, without increasing protection against the improper use of synthetic content that depicts individuals and is distributed for prohibited purposes.

PERFORMANCE IMPLICATIONS

ADMINISTRATIVE IMPLICATIONS

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

House Bill 221 is related as it provides the many of the same protections as HB 401
House Bill 60 and House Bill 410 are also related. These bills define many of the same terms differently, creating potential conflict and ambiguity that could impede compliance.

TECHNICAL ISSUES

OTHER SUBSTANTIVE ISSUES

ALTERNATIVES

Expressly exempt state agencies and public bodies as state agencies and public bodies will not be using AI systems to produce content that depicts individuals and distributing such content for improper purposes.

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

AMENDMENTS

Add an explicit exemption for state agencies, public bodies, and political subdivisions of the state.