LFC Requester:	**Hilla**

AGENCY BILL ANALYSIS - 2026 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: *1/24/2026* *Check all that apply:*
Bill Number: *SB 68* Original *X* Correction __
Amendment ___ Substitute ___

Sponsor: Berghmans
Short Title: Artificial Intelligence Government Act

Agency Name and Code Number: Office of Cybersecurity
Person Writing Analysis Todd Baran
Phone: 505.231.3990 **Email** Todd.baran@cyber.nm.gov

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

Appropriation		Recurring or Nonrecurring	Fund Affected
FY26	FY27		
0	0	NA	NA

REVENUE (dollars in thousands)

Estimated Revenue			Recurring or Nonrecurring	Fund Affected
FY26	FY27	FY28		
0	**0**	**0**	NA	NA

(Parenthesis ( ) indicate revenue decreases)

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY26	FY27	FY28	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total	0	0	0	0	NA	NA

(Parenthesis ( ) Indicate Expenditure Decreases)

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

SECTION III: NARRATIVE

BILL SUMMARY

Section 1 of SB68 would enact the "Artificial Intelligence Government Use Act."

Section 2 would provide definitions for key terms as follows:

- **Artificial Intelligence:** Machine-based system that can infer from input and generate outputs influencing environments.
- **Automated Decision Tool:** AI system designed or modified to make decisions or generate scores, labels, predictions, or recommendations that influence decisions.
- **Consequential Decision:** Decisions with significant legal or material impact on education, employment, finance, housing, healthcare, insurance, or legal services.
- **Cybersecurity:** Practices to reduce risk of data loss, breaches, or reputational harm.
- **Nonpublic Data:** Confidential information legally protected from disclosure.
- **Public Body:** State agencies, local governments, school districts, charter schools, and public post-secondary institutions.
- **Technology Resource:** Hardware, software, infrastructure, or personnel used for automation, communication, or data processing.

Section 3 would require every public body to establish AI governance policies that address:

- Authorized uses of AI, automated decision tools, and technology resources.
- Security procedures for protecting nonpublic data.
- Definitions of authorized use for AI and automated tools.
- Mandate that a human employee makes the final consequential decision, regardless of AI recommendations.
- Prohibition against using AI or tech resources to override security or system integrity procedures (except authorized testing).

Policies must be made available to the public upon request.

Section 4 would require every public body to train employees on:

- Cybersecurity and AI/automated tool policies.
- Appropriate use of AI and automated decision tools in decision-making.

Under Section 5, the Act would become effective July 1, 2026.

FISCAL IMPLICATIONS

No notable fiscal implications for OCS. Some public bodies may incur increased costs for contracted professional services required to support policy development, such as outside legal counsel or IT expertise.

Note: major assumptions underlying fiscal impact should be documented.

Note: if additional operating budget impact is estimated, assumptions and calculations should be reported in this section.

SIGNIFICANT ISSUES

Smaller entities may lack expertise or resources to draft comprehensive policies, particularly on specialized issues such as AI ethics, cybersecurity, and authorized use. Entities without in-house policy development expertise may need to contract for policy development professional services, or may forego developing a policy or adopting AI to avoid the compliance burden. This could adversely impact constituent services that would otherwise be supportable by AI.

Mandating development of entity specific policies risks fragmentation or inconsistent policies. Definitions and standards may vary widely, creating compliance confusion.

Mandatory training for all employees adds cost and logistical complexity. These burdens can be mitigated by mandating that public entities participate in AI training currently offered by the Office of Cybersecurity.

Individualized cybersecurity and data governance policies may conflict with standards and best practices specified by the Cybersecurity Advisory Committee, and be redundant of standard development work of the Committee. The Committee recently authorized a policy development project to create a policy library accessible by all public entities. Requiring public bodies to develop individual policies while that project is in process may result in wasted effort by local public bodies or the Committee.

Mandating that policies be available to the public may reveal cybersecurity sensitive information that is otherwise protected by IPRA. To ensure harmony between the Act and IPRA exceptions, the Act should clarify that existing and future IPRA exceptions supersede the disclosure requirement.

PERFORMANCE IMPLICATIONS

ADMINISTRATIVE IMPLICATIONS

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

TECHNICAL ISSUES

OTHER SUBSTANTIVE ISSUES

ALTERNATIVES

Mandate adoption of template policies and training by public bodies: The Cybersecurity Advisory Committee, in coordination with the Office of Cybersecurity, is developing a cybersecurity policy template library for local governments. This library will include policies on AI security, and can be expanded to include policies on AI governance and ethics. Widespread adoption of standardized policies would promote consistent levels of AI security, governance and ethics throughout state government, minimize the policy development burden on smaller public bodies and streamline compliance and oversight and personnel move between public entities.

The Office of Cybersecurity also offers AI awareness training to all public bodies. Mandating participation in a standardized training program will lower overall costs to the state, and ensure equality of content for all public entities.

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

Policy development will continue on an ad hoc basis, and AI may be deployed in the public sector without appropriate, or any, governance.

AMENDMENTS

* This document was drafted with the assistance of the Co-Pilot artificial intelligence tool. The final content has been thoroughly reviewed, edited, and approved by Raja Sambandam, Chief Information Security Officer, and Todd Baran, General Counsel, to ensure content accuracy, legal compliance, and subjectivity.