LFC Requester:	Malone

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: *2/7/2026*
Bill Number: *HB202*

Check all that apply:
Original *X* Correction __
Amendment __ Substitute __

Sponsor: Dow and Armstrong
Short Title: Child Advocate Office Data Sharing

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**		
75 to OCA		N	GF

REVENUE (dollars in thousands)

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

(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	15	25	25	65	R	GF

(Parenthesis ( ) Indicate Expenditure Decreases)

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

SECTION III:

BILL SUMMARY

Synopsis:

Section 1 – New Material: Multi-Agency Memorandum of Understanding (MOU)

- **Purpose:** Requires the Office of Child Advocate (OCA) and seven state agencies to enter into a single multi-agency MOU for sharing data and systems access.
- **Agencies involved:**
    1. Administrative Office of the Courts
    2. Children, Youth and Families Department
    3. Department of Health
    4. Department of Public Safety
    5. Early Childhood Education and Care Department
    6. Health Care Authority
    7. Public Education Department
- **Collaboration:** Department of Information Technology (DoIT) and Attorney General assist in drafting and execution.
- **Working Group:**
    1. Convened by June 15, 2026
    2. Includes representatives from OCA, each agency, AG, and DoIT staff
    3. Must finalize and execute MOU by October 15, 2026
- **MOU Requirements:**
    1. Identify data and system access levels
    2. Define sharing/storage methods and platforms
    3. Security protocols, audit logging, breach plan
    4. Oversight and reporting requirements
    5. Compliance with HIPAA, FERPA, court rules, and DoIT cybersecurity standards
    6. Legal and technical review by all parties
- **Reporting:** Copies of executed MOU to Legislative Finance Committee, Governor, and Legislative Health and Human Services Committee by Nov 1, 2026.

Section 2 – Appropriation

- **Amount:** $75,000 from the general fund to OCA for FY2026–2027
- **Purpose:** Technical services to implement the Act
- **Reversion:** Unspent funds revert to the general fund at end of FY2027.

FISCAL IMPLICATIONS

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.

As explained below in Significant Issues, the Office of Cybersecurity (OCS) has a statutory responsibility to ensure that data sharing protocols and processes for state agencies meet minimum standards established by law and policy. OCS estimates that staff time to perform these planning and oversight functions will amount to approximately $25K per-year, after FY26. FY26 staffing

spend is estimated to be approximately $15K.

SIGNIFICANT ISSUES

OCS is an independent agency vested with the statutory authority and obligation to "develop and implement cybersecurity policies, standards and guidelines for state agencies." NMSA § 9-27A-3(A). OCS is also responsible for "coordinating cybersecurity efforts among state agencies." NMSA § 9-27A-4(A)(1). HB202 requires:

- Cybersecurity measures and protocols for data/system sharing (Section 1(D)(4)).
- Audit logging and breach plan (Section 1(D)(5)-(6)).
- Compliance with cybersecurity requirements (Section 1(D)(8)(e)).

These responsibilities fall squarely within the Office of Cybersecurity's statutory mandate to ensure statewide cybersecurity compliance, including:

- Proper alignment with state cybersecurity standards.
- Risk mitigation for sensitive child welfare, health, and education data.
- Efficient breach response planning.

Although the MOU and data sharing plan contemplated by HB202 will require compliance with OCS mandates, and collaboration with OCS security operations, OCS is not included in the stakeholder group that will develop the MOU. This could result in conflict between MOU terms and OCS standards and security operations. To help prevent misalignment of MOU terms and cybersecurity compliance and ensure that all relevant cybersecurity concerns are addressed by the MOU, HB202 should be amended to include OCS in the MOU stakeholder development group. This will help ensure that relevant cybersecurity standards are considered and applied to sensitive child welfare, health, and education data.

PERFORMANCE IMPLICATIONS

ADMINISTRATIVE IMPLICATIONS

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

Section 1(D)(8) (e) of the bill requires the data sharing MOU to require the data sharing platform to comply with "operational and cybersecurity requirements or recommendations of the department of information technology." As noted above, NMSA § 9-27A-3(A) vests OCS with authority to set cybersecurity standards for state agencies. Because OCS, not the department of information technology, sets cybersecurity standards for state agencies, HB202 conflicts with existing law and will unnecessarily complicate MOU development and implementation by requiring agencies to comply with both OCS and otherwise non-binding cybersecurity standards of the department of information technology.

TECHNICAL ISSUES

OTHER SUBSTANTIVE ISSUES

The MOU that is the subject of this bill will facilitate sharing of some of the most sensitive and protected records managed by public agencies. This includes health records, student records and child welfare records, all of which are protected by law.

Facilitating the exchange of these records and information amongst agencies with common interests will increase government efficiency, minimize errors, eliminate redundances and improve constituent services. However, whenever information technology systems are configured to facilitate record sharing and information exchange, the risk of a data-breach increases. Where before it may only have been necessary to safeguard records in one repository, the contemplated sharing will require sensitive records to be protected in multiple repositories, and while in transit. Every repository and every network over which records are shared is a potential point of cyber-attack that must be defended. Failure to do so could result in a catastrophic disclosure of sensitive information that can disrupt lives through invasion of privacy, identity theft, loss of physical security and financial manipulation. The economic cost to the state of any such breach may run into millions of dollars. The emotional, financial and other impacts on the persons whose information is disclosed is incalculable.

HB202 recognizing the importance of cybersecurity to the success of the MOU. To ensure all cybersecurity risks are fully identified and addressed, the Office of Cybersecurity should participate in this important initiative.

ALTERNATIVES

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

AMENDMENTS

Amend Section 1, subsection A to read as follows:

. . .

(6) the health care authority; ~~and~~
(7) the public education department; and

(8) the cybersecurity office.

Amend Section 1(D)(8) (e) of the bill to read "operational and cybersecurity requirements or recommendations of the Cybersecurity Office ~~department of information technology~~."