LFC Requester:	Hilla

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: 2/21/2025
Bill Number: HB 497

Check all that apply:
Original __X__ Correction ____
Amendment ____ Substitute ____

Sponsor: Brown

Agency Name and Code Number: 361 – DoIT

Person Writing Analysis: Todd Baran

Short Title: Inspection of Public Records Act Changes

Phone: 505-231-3990 **Email:** Todd.baran@doit.nm.gov

SECTION II: FISCAL IMPACT

APPROPRIATION (dollars in thousands)

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

(Parenthesis ( ) indicate expenditure decreases)

REVENUE (dollars in thousands)

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

(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						

(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

Synopsis: House Bill (HB) 497 would amend the Inspection of Public Records Act (IPRA) to expand exemptions, revise deadlines, designate additional records as law enforcement records, provide additional definitions, revise the procedures for requesting and denying requests for public records, and revise provisions related to enforcement.

Section 1 of HB 497 would amend IPRA exemptions, as follows:

- Change, "records pertaining to physical or mental examinations and medical treatment of persons confined to an institution" to "medical records."
- Add an exemption for letters of reference concerning procurement.
- Expand the exemption for letters or memoranda that are matters of opinion in a personnel file or students' cumulative files, to include "the reports, notes and evidence generated by internal investigations of personnel or students."
- Create an exemption for, "a person's personal email address or personal telephone number that is provided to a public body for the purpose of communications with the public body or in connection with the person's application for a permit or license; provided, however, that the person's identity shall not be withheld."
- Create an exemption for, "security system records of a public body's facility, the disclosure of which would reveal information that could be used to plan or execute an attack on a public facility or a person."
- Create an exemption for, "records that relate to cybersecurity information or critical infrastructure, the disclosure of which could expose the related systems to vulnerabilities or could jeopardize the safety of critical infrastructure systems."
- Create an exemption for, "a public body's security system plan and records regarding: disaster mitigation, preparation, response, vulnerability or recovery; and cybersecurity planning or threat mitigation."
- Create an exemption for, "security codes, passwords and lock combinations or plans used to protect a public body's electronic information or to prevent improper access to the public body's computers, computer systems and computer and telecommunications networks."
- Create an exemption "when a public body seeks to acquire real property by purchase or through the exercise of the power of eminent domain, all appraisals and reports relating to value, offers and counteroffers on the real property until a valid option contract has been executed or a written offer to sell has been conditionally accepted by the public body, at which time this exception to inspection shall expire."
- Create an exemption for, "records submitted to a public body by a bidder on a public contract that relate to the financial stability of the bidder, including tax returns, financial statements and bank statements."
- Create an exemption "before a contract is awarded, materials submitted in response to a sealed bidding or request for proposals issued by a public body."
- Create an exemption for, "customer records for utility services provided by a public body, including the customer's billing statements, records of consumption or usage, payment

information or methods and the contents of any customer communications made in connection with the customer's utility services."

- Create an exemption for, "records that may disclose or lead to the discovery of the identity of a person who made a report of alleged abuse, neglect or exploitation of a child or of a protected adult as defined in Section 27-7-16 NMSA 1978."
- Create an exemption for, "records concerning an individual applicant for or recipient of unemployment insurance or economic assistance or support, including applications, income or eligibility verification, assessments and other personal medical or financial data related to the insurance, assistance or support."
- Create an exemption "with respect to a request for records received from a person who has been convicted of an indictable offense under the laws of this state, another state or the United States and that relates to the victim of the offense for which the person was convicted, personal information pertaining to the crime victim or the victim's family, including the victim's home address, home telephone number, personal telephone number, work or school address and telephone number, social security number, medical history or any other identifying information."

Section 2 would amend IPRA exemptions for law enforcement records. It removes the language stating, "that the presence of nonpublic information may be redacted from a written record or digitally obscured in a visual or audio record." It would add a provision state that, "if a law enforcement agency becomes aware of a crime to which a request for law enforcement records relates, the time for responding to that request for law enforcement records is tolled for forty-five days immediately following the day on which the law enforcement agency becomes aware of the crime." It expands exemptions to the following:

- The names, addresses, contact information, protected personal identifier information, and other identifying information of individuals who are victims of or non-law-enforcement witnesses to an alleged crime of:
    - kidnapping pursuant to Section 30-4-1 NMSA 1978;
    - abandonment of a child pursuant to Section 30-6-1 NMSA 1978;
    - abuse of a child pursuant to Section 30-6-1 NMSA 1978;
    - abandonment of a dependent pursuant to Section 30-6-2 NMSA 1978;
    - enticement of child pursuant to Section 30-9-1 NMSA 1978;
    - voyeurism pursuant to Section 30-9-20 NMSA 1978;
    - incest pursuant to Section 30-10-3 NMSA 1978;
    - child solicitation by electronic communication device pursuant to Section 30-37-3.2 NMSA 1978;
    - criminal sexual communication with a child pursuant to Section 30-37-3.3 NMSA 1978;
    - unauthorized distribution of sensitive images pursuant to Section 30-37A-1 NMSA 1978;
    - abuse pursuant to the Resident Abuse and Neglect Act; and
    - human trafficking pursuant to Section 30-52-1 NMSA 1978.
- The name, address, contact information, protected personal identifier information and other identifying information of a juvenile and of the juvenile's parent or guardian, when the juvenile is a victim of or witness to a crime or an alleged crime.
- Any information that would identify or provide a means of identifying a confidential informant of a law enforcement officer or prosecutor, if the identity of the informant is not otherwise publicly known, is exempt from inspection.
- The work schedule of an employee of a law enforcement agency or correctional facility is

exempt from inspection.

- Records and other information that would reveal the identity or endanger the life or safety of an undercover law enforcement officer are exempt from inspection.
- Audio recordings, video recordings and images taken with a law enforcement officer's body-worn camera or similar device, if the recordings or images are taken in a private place, are exempt from inspection, except for recordings, images or records that:
    - depict the commission of an alleged crime;
    - record an encounter between a law enforcement officer and a person that results in the death or bodily injury of a person, or includes or captures a law enforcement officer firing or discharging a weapon; or
    - record an encounter that is the subject of a current legal proceeding against a law enforcement officer or law enforcement agency.

Section 3 adds new definitions for the following:

- "broad or burdensome" means a request that requires a public body to spend more than three hours to locate the public record and redact information exempt from inspection.
- "critical infrastructure" means public buildings; systems, including telecommunications centers and computers; power generation plants, dams, bridges and similar resources; systems related to utility services, fuel supply, energy, hazardous liquid, natural gas or coal, whether physical or virtual; such that the incapacity or destruction of the infrastructure would have a debilitating impact on security, economic security, public health or safety.
- "current records" means public records that were created or received by a public body within the twelve months preceding receipt of a request to inspect the records, but does not include archival records.
- "cybersecurity information" means information related to acts, practices or systems that eliminate or reduce the risk of loss of critical assets, loss of sensitive information or reputational harm as a result of a cyber attack or breach within an organization's network.
- "good faith" means:
    - when conducting a search in response to a request for inspection, making reasonable efforts to determine from a public body's officials or employees whether a requested record exists and, if it does, how the record can be inspected; and
    - when denying inspection, reasonably relying on statutes, decisions of a court, advice of counsel, guidance issued by the attorney general and public policy.
- "law enforcement records" means evidence, in any form, received or compiled in connection with a criminal investigation or prosecution by a law enforcement or prosecuting agency, including inactive matters or closed investigations to the extent that the records contain the information described in Section 14-2-1.2 NMSA 1978; provided, however, that the presence of such information on a law enforcement record does not exempt the record from inspection.
- "medical records" means any information, whether oral or recorded in any form or medium, related to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or past, present or future payment for the provision of health care to an individual.
- "person" means any individual, corporation, partnership, firm, association, [or] entity or public body domiciled in New Mexico, but does not include an individual incarcerated in a correctional facility.
- "private place" means the interior of a residence, the interior of a facility that offers health care, or social services or another interior place that is not open to members of the public and inside of which a person has a reasonable expectation of privacy.

- Removes the qualifier that all but the last for digits of social security number, tax payer identification number, date of birth, etc. are public records.
- Expands exemptions for the following information with regard to a nonelected employee of a public body in the context of the person's employment:
    - the employee's home telephone number or personal cellular phone number;
    - the employee's personal email address;
    - the employee's payroll deduction information; and
    - the name, address, telephone number and contact information of any dependent or emergency contact of the employee.
- "reasonable denial", with respect to a denied request to inspect public records, is one that provides:
    - a reason supported by the Inspection of Public Records Act; another state, federal, or local law or rule; or a ruling or decision of a court or a court order to justify why a record is exempt from inspection, regardless of whether a precise legal citation is provided; or
    - a reasonable justification, based on a public policy, for refusing to release the records.
- "reasonable particularity" does not include a request that seeks records by identifying search terms or parameters that a public body does not use to index, organize, file or record its records or that cannot be used to search those records, but does mean to identify specific records by:
    - in the case of records other than audio or visual records, providing at least two of the following:
        - the record title or subject line;
        - the author; or
        - the applicable date or date range, with reasonable specificity; or
    - in the case of audio or visual records, providing at least one of the following:
        - the computer-aided dispatch record number;
        - the police report number; or
        - the applicable date or date range with reasonable specificity and at least one of the following: 1) the name of a law enforcement officer or first responder; 2) the approximate time or the approximate location; or 3) other criteria established and published by a public body to facilitate access to videos.
- "utility services" means those services, when performed by a public body, that would constitute a public utility as defined by Section 62-3-3 NMSA 1978, a public telecommunications service as defined by Section 63-9A-3 NMSA 1978 or a cellular service company as defined by Section 63-9B-3 NMSA 1978, and includes services provided by associations as defined under the Sanitary Projects Act.

Section 4 would amend the requirements for requesting records, as follows:

- If a request is sent to a person other than the appropriate custodian, the time for fulfilling the request shall be tolled until the request is delivered to the appropriate records custodian. All employees or agents of public bodies shall promptly forward to the appropriate custodian any requests misdirected to the employee or agent.
- Nothing in IPRA would be construed to require a public body to:
    - create or maintain a public record;
    - compile, format, manipulate, package, summarize or tailor information in response to a request;
    - provide a record in a particular format or medium not currently maintained by the

public body
    - provide a record that is included in a report or document that is printed or published, including a document that is available on the internet; or
    - answer questions, conduct research, provide advice or issue legal opinions.
- Require written requests, to include the actual name, mailing address, telephone number and email address of the person seeking access to the records. Anonymous or pseudonymous requests shall not be submitted, and a public body shall not be required to respond to such requests. If a request is made by an agent for another person, the agent shall disclose the name of the person on whose behalf the agent is acting.
- Increase the time for record custodians to reply to a request from fifteen to twenty-one business days after receiving a written request in the case of current records or sixty business days in the case of records that are not current records or are audio or visual records.
- Add a provision stating that a request submitted outside of the public body's business hours shall be considered submitted during the business day following submission of the request, for purposes of calculating deadlines.
- Allow written requests to include a communication using an internet process that is provided by the public body.
- A public body may ask a requester to clarify a request.
- A public body may discuss with a requester of a large volume of records how the scope of a request may be narrowed.
- With regard to electronic records:
    - nothing in this section requires a public body to attempt to recover or restore deleted or overwritten records; and
    - nothing in this section requires a public body to provide inspection of browser histories, caches, cookies, file metadata, system logs, login histories or internet protocol addresses of visitors to the public body's websites.
- The time limits for a public body to allow a person to inspect records relating to elections shall be tolled during the period beginning on the fifty-sixth day prior to an election until the canvass of the election has been certified by the county canvassing board or state canvassing board, whichever is later.

Section 5 amends the procedures for inspecting records to:

- Increase the fee from $1 to $2 per printed page.
- Allow a custodian to:
    - charge a fee not exceeding thirty dollars ($30.00) per hour per request, excluding the initial three hours, for the time required to locate and redact records;
    - if a person makes five or more requests within a forty-five-day period, treat the requests as one request in computing the time for labor charges;
    - allow a person to use the person's own personal devices for duplication of records and shall establish reasonable procedures to protect the integrity of the records; provided that the procedures are not used to prevent access to the records; and
    - decline to provide an opportunity to inspect a record to a person who has already inspected that same record.

Section 6 amends the procedures for denied requests, as follows:

- Increase the time for deeming a request denied from fifteen to twenty-one days.
- Only allow the requester to pursue remedies, after providing the public body from which the public record was requested with written notice of the claimed violation. Once the

public body has received the written notice, the public body shall have twenty-one calendar days to respond to the written notice and twenty-one calendar days to remedy the violation. After the two twenty-one-calendar-day periods have elapsed, the public body shall be subject to enforcement as provided in Section 14-2-12 NMSA 1978.

Section 7 amends the enforcement of IPRA as follows:

- Only allow enforcement after a public body has received written notice of a claimed violation of the Inspection of Public Records Act and has failed to respond within twenty-one business days.
- Actions to enforce the Inspection of Public Records Act shall be brought exclusively against the public body in the district court in the county where the public body maintains its principal office. No records custodian or other employee or official of the public body may be named as a defendant.
- Any public body named in an action filed pursuant to the Inspection of Public Records Act shall be held liable for conduct of individuals acting on behalf of, under color of or within the course and scope of the authority of the public body.
- Actions to enforce the Inspection of Public Records Act shall be exclusively brought as a civil action and proceed under the rules of court for civil complaints. The district court shall not issue peremptory writs of mandamus or alternate writs of mandamus under Section 44-2-7 NMSA 1978.
- Allow a district court to issue a writ of mandamus or order an injunction or other appropriate remedy only after:
    - the public body has been served with a summons and a complaint;
    - the public body has given due process in accordance with the rules of civil procedure; and
    - the court has found that the public body failed to produce records in violation of that act.
- Limit an award of damages, costs, and attorney fees only in cases where the public body did not act in good faith or failed to provide a reasonable denial.

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.

By expanding exemptions, providing additional time to collect records over one-year old, defining "broad and burdensome" in a manner that allows an agency time to conduct normal operations while still responding to an IPRA request, circumscribing the scope of required searches by establishing good faith and reasonableness standards, and protecting public bodies from abusive requesters, DoIT would likely realize a significant reduction in costs for IPRA compliance. DoIT estimates it would save the equivalent of at least 1 FTE per-fiscal year.

SIGNIFICANT ISSUES

- DoIT and the Office of Cybersecurity (OCS) generate and collect a significant number of records, the disclosure of which could facilitate a cyber attack on state owned information technology systems. Under current law, such records cannot be withheld unless they reveal

information that would compromise an information technology system. This standard allows DoIT to withhold cybersecurity vulnerability information that, standing alone, would place a system at risk, but could be construed to require production of records that would only reveal a component of information required to compromise an IT system. Cybersecurity breaches often result from the collection of disparate pieces of information that, when consolidated by a malicious actor, reveals a vulnerability in an IT system. Under the proposed exemption for "records that relate to cybersecurity information or critical infrastructure, the disclosure of which could expose the related systems to vulnerabilities or could jeopardize the safety of critical infrastructure systems", which is operationalized by a broad definition of "cybersecurity information", DoIT would be able to withhold records that would establish a link in the chain of information required to compromise a system. This would allow DoIT and the OCS to more effectively protect the state's information technology systems and sensitive data in those systems.

In addition to expanding the category of exempt cybersecurity sensitive records, HB497 would resolve numerous compliance challenges for DoIT. Most significantly, DoIT would have recourse when it receives records requests from an abusive requester. For the past several years, DoIT has been managing a string of requests from an individual who is hostile, abusive and threatening. Providing a mechanism to avoid interactions with such requesters will promote the wellbeing and safety of DoIT's dedicated IPRA staff.

HB497 would also minimize IPRA compliance burdens by extending time to locate aged records. As modern IT systems facilitate storage of more records for longer periods of time, current IPRA compliance often requires DoIT to search increasingly large volumes of records dating back years, and often far beyond existing retention schedules. Agencies often retain records longer than required by law to facilitate institutional knowledge and operational efficiency. Under current law, DoIT is required to search through and produce responsive records from these collections under the same time limits that apply to records more recently created or collected. HB497 would allow more time to search for and produce aged records. HB497 would also reduce IPRA compliance burdens by enacting common sense definitions of "reasonable denial", "good faith" and "broad and burdensome."

HB497 would also facilitate IPRA compliance and minimize burdens by adding a commonsense definition of "reasonable particularity". Under the proposed definitions, vague and subjective requests, such as a request for records relating to an assumed set of facts or circumstances, would not trigger a compliance obligation. A request would need to be objectively clear as to what records would be responsive. The proposed law would also expressly allow a public body to engage in an interactive process with a requester to refine the subject of a search. These proposed improvements would eliminate the frequent need for DoIT to try and postulate whether a record is responsive to the request, which often results in an over-production of records creating an undue burden for both DoIT and the requester.

PERFORMANCE IMPLICATIONS

ADMINISTRATIVE IMPLICATIONS

CONFLICT, DUPLICATION, COMPANIONSHIP, RELATIONSHIP

TECHNICAL ISSUES

OTHER SUBSTANTIVE ISSUES

HB457 would define "reasonable denial" to include a denial "based on a reasonable justification, based on a public policy, for refusing to release the records." This language strongly implies that there is a "public policy" IPRA exception. However, no such exception appears in the express exceptions identified in Section 1 of the bill. This ambiguity should be resolved by adding an explicit public policy exception to IPRA to support the reference to "public policy" in the definition of "reasonable denial".

- HB457 would create an exception for "security codes, passwords and lock combinations or plans used to protect a public body's electronic information or to prevent improper access to the public body's computers, computer systems and computer and telecommunications networks." Any such records would be covered under the general exception for records that would expose a cybersecurity vulnerability, creating a redundancy and potential ambiguity. If this exception was intended to encompass something other than a record showing a cybersecurity vulnerability, it should be clarified.

HB457 would require a public body to allow a person to use the person's own personal devices for duplication of records and shall establish reasonable procedures to protect the integrity of the records; provided that the procedures are not used to prevent access to the records. This provision will be exceptionally difficult to implement because allowing unknown devices to connect to a state information technology network is, by definition, a cybersecurity vulnerability and expressly prohibited by DoIT rule. The only practical way to implement this provision without creating a cybersecurity vulnerability would be for each public body to maintain at least one computer that does not connect to a network and is reset to factory settings after each time an unknown device is connected to that computer. Without conducting such a reset, an air-gapped computer can spread a virus loaded by the unknown device if a user re-uses any portable media that was ever connected to the device. It is impractical to implement such practices consistently. Therefore, public bodies should not be required to allow connections of unknown devices.

HB457 provides that a public body that produces electronic records is not required to provide inspection of browser histories, caches, cookies, file metadata, system logs, login histories or internet protocol addresses of visitors to the public body's websites. This language arguably conflicts with the language in Section 5 of the bill which requires a public body to "provide a copy of a public record in electronic format if the public record is available in electronic format and an electronic copy is specifically requested." The latter language implies that a public body must produce electronic records in native format if requested. Because native file formats include metadata, allowing a public body to withhold metadata conflicts with the direction to provide native electronic files. For clarity, the bill should be clarified to expressly define a "record" to exclude browser histories, caches, cookies, system logs, login histories or internet protocol addresses of visitors to the public body's websites.

ALTERNATIVES

Instead of requiring public bodies to allow connections of unknown devices, the bill could be revised to allow photographic scanning of documents by a user who does not want physical or electronic copies of responsive records.

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

Public bodies will continue to receive and process vague and burdensome record requests, have no recourse against abusive IPRA requesters, and could only rely on a limited set of exceptions that fail to protect vast amounts of sensitive information, much of which relates to individuals and personal privacy.

AMENDMENTS