FISCAL IMPACT REPORT

SPONSOR HJC **LAST UPDATED**
ORIGINAL DATE 03/08/23
BILL NUMBER CS/House Bill 232/ec/aHCPAC/HJCS
SHORT TITLE Disclosure of Certain Info
ANALYST Hitzman

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT*
(dollars in thousands)

	FY23	FY24	FY25	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
	Indeterminate but minimal	Indeterminate but minimal	Indeterminate but minimal		Recurring	General Fund

Parentheses ( ) indicate expenditure decreases.
*Amounts reflect most recent analysis of this legislation.

Relates to HB251

Sources of Information

LFC Files
National Governor's Association
Inspection of Public Records Compliance Guide - AG

Response (to Original Bill) Received From
Department of Information Technology (DoIT)
Commission of Public Records
Public Regulation Commission (PRC)
Department of Transportation (NMDOT)
Office of Attorney General (NMAG)
State Land Office (SLO)

SUMMARY

Synopsis of HJC Substitute for House Bill 232

The House Judiciary Committee substitute for House Bill 232 (HB232) adds new material to the Tourism Department Act to exempt from public records inspection the proprietary technical or business information relevant to specific marketing or advertising campaigns for the state and consumer's individually identifiable information provided during online, tourism–related transactions.

The bill amends and adds a new section to the Inspection of Public Records Act to exempt portions of law enforcement records. The bill provides that law enforcement records are public records provided that nonpublic information is redacted, including:

- Names, address, contact information or protected personally identifiable information (PII) of victims and non-law enforcement witnesses before charges are filed for crimes of assault against a household member with intent to commit a violent felony, stalking, aggravated stalking, criminal sexual penetration, criminal sexual contact, and sexual exploitation of children.
- Names, address, contact information or PII of individuals accused but not charged with a crime,
- Visual depictions of a dead body unless an officer is alleged or suspected to have cause the death,
- Visual depictions of great bodily harm unless an officer is alleged or suspected to have cause the harm,
- Visual depictions of an individual's intimate body parts,
- Visual or audio depictions of the notification of a member of the public of a family member's death,
- Confidential sources, methods, or information, or
- Records pertaining to physical or mental examination and treatments of persons unless relevant to a criminal investigation.

The bill specifies the required information to include in a request for release of audio or video, including at least one of the following: the computer-aided dispatch record number, police report number date or date range and the name of the officer or responder, the approximate time and approximate location. A request to view video or hear audio on-site of a public body is not subject to the restrictions.

The bill provides a definition of "law enforcement record" that includes evidence in any form, including closed investigations.

The bill also exempts information concerning information technology (IT) systems that would reveal specific vulnerabilities that compromise or allow unlawful access. However, the section shall not be used to restrict access to records stored or transmitted using IT systems internal and external audits of IT systems, or information to authenticate or validate records received pursuant to a request fulfilled pursuant to IPRA. The bill also exempts submissions in response to competitive grants, and leases, and scholarships and related scoring materials and evaluations reports until finalists are publicly named.

The bill provides a new definition for "information technology systems," meaning computer hardware, storage media, networking equipment, physical devices, infrastructure, processes and code, firmware, software, and ancillary products and services. Regarding the definition of PII, the bill adds all but the last four digits of a credit and debit card number and the employee's nonbusiness home street address for nonelected employees of a public body.

This bill contains an emergency clause and would become effective immediately on signature by the governor.

FISCAL IMPLICATIONS

The bill does not contain an appropriation but is expected to have an indeterminate but likely minimal fiscal impact. As noted by the Department of Transportation (NMDOT), "given the new

exceptions relevance to NMDOT's field of regulation, NMDOT may face increased litigation costs from IPRA-related suits as the courts define the contours of this new exception. However, it is impossible to determine how much these costs may be at this time."

SIGNIFICANT ISSUES

The substituted bill includes "infrastructure" within definition of IT systems, but it does not specify the type of infrastructure. New Mexico is one of 19 states that have no exemption for critical infrastructure information. Colorado, for example, passed legislation in 2017 that exempts certain information about state critical infrastructure from the Colorado Open Records Act to increase infrastructure security.

The Department of Information Technology (DoIT) notes:

> Under current law, public records consisting of strategic defense plans and assessments regarding IT systems and infrastructure are exempt from disclosure under IPRA. However, no law protects the source documents and records that contain information used to compile those plans and that reveal vulnerabilities. This proposed law would exempt source documents from inspection under IPRA if the source records contain information that could expose a vulnerability in an IT system or critical infrastructure. Notably, other states have similarly broad exemptions relating to public safety. *See, e.g.*, Mich. Comp. Laws Serv. § 15.243(1)(y); Wash. Rev. Code Ann. 42.56.420; Mass. Gen. Laws Ann. ch. 4, § 7(n).

To this end, the State Land Office (SLO) also previously noted that:

> The State Land Office and other state agencies have been subjected to public records requests seeking sensitive information about its computer systems, including software coding and network architecture. Arbitrary disclosure runs counter to minimum data security practices because such information can be utilized by hackers to penetrate and compromise computer systems. The bill has its roots in existing law. The New Mexico Administrative Code, 1.12.20.23 NMAC and 1.12.20.24 NMAC, affirmatively mandates that state computer systems be scanned and penetration-tested to proactively identify and correct cybersecurity vulnerabilities. Section 1.12.20.24 (F) NMAC mandates that results of such tests be "protected from public disclosure." Revelation of this information to a public records requester would defeat the entire purpose of those basic and essential cybersecurity measures.
>
> Sensitive details about utilities are also protected by this bill. Hb 232 is in conformity with the federal mandate from the Department of Energy to harden domestic utility computer systems to avoid cyberattacks. *See* "Building a Better Grid Initiative to Upgrade and Expand the Nation's Electric Transmission Grid to Support Resilience, Reliability, and Decarbonization" initiative. Department of Energy, 87 Fed. Reg. 2769, 2769-2773 (Jan. 19, 2022).
>
> At the same time, disclosure of sensitive details regarding the operation of essential utilities, or the inner workings of state-operated computer systems, does nothing to deprive the public of meaningful information about the workings of government "and the official acts of public officers and employees," NMSA 1978, § 14-2-5, which is the statutory purpose of IPRA.

The substituted bill provides additional clarity by providing a definition of "information technology system."

In its *Inspection of Public Records Act Compliance Guide*, the Attorney General's Office (NMAG) noted that, under existing law:

> [The law enforcement] exception does not protect all records held by a law enforcement agency. The exception applies only to records that are (1) created or used by a law enforcement agency in connection with a criminal investigation or prosecution and (2) reveal confidential sources, methods, information or individuals accused but not charged with a crime. Generally, the records that fall within the exception's protection are those that, if made public, would seriously interfere with the effectiveness of a criminal investigation or prosecution….
>
> Whether a law enforcement agency can deny inspection of a particular record may depend on the phase of the criminal investigation or prosecution. For example, the name of a suspect will no longer be covered by the exception if the person is charged with a crime. However, if the target of an investigation or a suspect is not charged, that person's identity can remain confidential even after the investigation is closed….

HB232 would expand the list of records that are exempt from inspection to include additional information about victims of certain crimes—particularly crimes involving stalking, assault, and sexual contact or exploitation—visual and audio depictions of harm, death, or body parts, and other records or depictions that could place a victim or their family members at risk of exploitation or further harm. These new exemptions cover additional records and information that could interfere with the effectiveness of an investigation and provides additional protections to victims without exempting records pertaining to offenses committed by officers, such as death or bodily harm, which can improve transparency regarding officer conduct. Further, requiring an individual to have information regarding the offense, such as a police report number, before information will be released regarding a victim or crime provides additional protections.

However, nothing in the bill seems to change the information protections regarding the Arrest Record Information Act:

> [Under existing law,] the law enforcement records exception does not protect information subject to disclosure under the Arrest Record Information Act (NMSA 1978, §§ 29-10-1 to -8). This includes records identifying a person who has been arrested. In addition, information contained in posters, announcements or lists for identifying or apprehending fugitives or wanted persons; court records of public judicial proceedings; records of traffic offenses and accident reports; and original records of entry compiled chronologically, such as police blotters, are required to be available for public inspection.

NMAG's Compliance Guide further notes, under existing law:

> In exceptional circumstances, information contained in an original record of entry or similar record might be redacted or blocked out before the record is disclosed in response to a public records request. Information may be withheld, however, only with substantial justification. For example, if a law enforcement agency knew or reasonably suspected that revealing a specific victim's address would put the victim's life in danger, then the agency could keep the address confidential.

HB232 explicitly provides that PII be redacted in certain instances before being released, which

strengthens the protections already in law without placing the burden on officers to determine whether or not disclosure of certain information would result in risk or danger to a victim. The bill instead provides a blanket protection of certain information and requires that information be redacted before being released.

However, by providing exemptions of additional records, there may be concerns regarding transparency and accountability regarding law enforcement activities. This may also be true of the exemptions for marketing and tourism-related information, but other states, such as Florida, also have these protections for trade secrets held by a county tourism promotion agency.

ADMINISTRATIVE IMPLICATIONS

If HB232 is passed, DoIT notes state entities subject to IPRA would need to be able to identify records that contain information about IT system and infrastructure vulnerabilities. It is unclear if this would result in additional administrative needs at agencies. For example, as noted by the Public Regulation Commission (PRC), the bill may result in additional review of IPRA requests and responses to ensure protected information is not provided for inspection.

The Commission of Public Records notes the bill will not likely result in additional administrative burden to the agency. Similarly, the State Land Office notes it "will not be required to expend staff resources reviewing and responding to requests for records on critical infrastructure or sensitive information technology systems."

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

Under current law, public records consisting of strategic defense plans and assessments regarding IT systems and infrastructure will continue to be exempt from disclosure under IPRA but not for the source documents and records that contain information used to compile those plans and that reveal vulnerabilities.

JH/al/ne/rl/ne