F I S C A L I M P A C T R E P O R T

SPONSOR Candelaria **ORIGINAL DATE** 2/6/18 **LAST UPDATED** **HB**

SHORT TITLE Public Disclosure of Cybersecurity Info **SB** 244

ANALYST Amacher

ESTIMATED ADDITIONAL OPERATING BUDGET IMPACT (dollars in thousands)

	FY18	FY19	FY20	3 Year Total Cost	Recurring or Nonrecurring	Fund Affected
Total	NFI	NFI	NFI	NFI		

(Parenthesis ( ) Indicate Expenditure Decreases)

SOURCES OF INFORMATION

LFC Files

Responses Received From
Attorney General's Office (NMAG)
Department of Information & Technology (DOIT)
Homeland Security & Emergency Management Department (HSEMD)
New Mexico Educational Retirement Board (ERB)
New Mexico Municipal League (NMML)
Secretary of State's Office (SOS)

SUMMARY

Synopsis of the Bill

Senate Bill 244 provides an exemption to the Open Meetings Act from public disclosure of certain information concerning cybersecurity. If enacted, the effective date of this bill is May 16, 2018.

FISCAL IMPLICATIONS

There are no known fiscal impacts.

SIGNIFICANT ISSUES

SB 244 provides an exemption in the Open Meetings Act from public disclosure of those portions of meetings addressing cybersecurity preparations against or expenses to cyberattacks or cyber threats if that discussion in an open meeting would prevent the public body engaging in it from effectively addressing cybersecurity issues, or implementing cybersecurity measures, or

otherwise would compromise the public body's network security.

OTHER SUBSTANTIVE ISSUE

The Open Meetings Act designates all meetings of any public body, except the legislature and the courts, as public meetings as governed by the provisions of the Act. This allows for the public to attend and listen to the discussions that support policy development and the means of which voting occurs in meetings of boards, commissions, administrative adjudicatory bodies, or other policymaking bodies of any state agency, or any agency or authority of any county, municipality, district or political subdivision. These public bodies, which have been tasked with the management and administration of certain functions and funds by the legislature, have a fiduciary duty to safeguard the confidential data of their membership and the accounts administered. However, because these public bodies are required to comply with the Open Meetings Act, discussions of cybersecurity of the respective agencies would be subject to public disclosure, and thereby providing information to potential bad actors possibly seeking to reveal weaknesses or exploit other aspects of the system.

All of the agencies that responded to the request for analysis of this bill expressed similar concerns relating to the position in which the public body is able to address cybersecurity effectively. As stated by NMML, in this day and age of aggressive cyberattacks against both large and small organizations it is imperative, in discussing matters of preparation for and response to cyber threats and attacks, that public agencies have the ability to protect those preparations or discussions. Possible disclosure of an organization's cyber network may provide the pathway for an attack by those seeking to do so.

NMAG points out that the proposed language of SB 244, as drafted, appears to only apply to the public body's own network security. It is not clear that the intent of the bill is to also apply to network security issues that may be otherwise associated with the public body but not in direct control. This may cause some confusion with interpretation if a public body has contracted with a third party for technical assistance but the projects are not a part of the public body's own network.

Additionally, NMAG notes that the proposed language allows public bodies to use a subjective interpretation with the specific applicability of the new exception. The exception provides that the exception only applies when such discussion "would" prevent the public body from effectively addressing a cybersecurity issue or "otherwise would compromise the public body's network security." While it could be debated that these elements are not satisfied in a specific instance, the Open Meetings Act does provide a legal presumption that a public body acted in accordance with the Act, which would help address this issue. See Section 10-15-3(A).

NMAG mentions that any votes or other action taken by a public body would still be required to take place in a public meeting, in open session and on record. Only the discussions of matters related to cybersecurity fall under the exception provided by SB 244.

NMHERB notes that if SB 244 is enacted, the public bodies could have discussions about preparations and responses to cybersecurity attacks and cyber threats disclosed in executive sessions. And would not have to produce minutes for those portions of meetings discussing cybersecurity. Such an exception would provide greater security for public agencies since they would be able to discuss in detail cyber preparations without revealing any weaknesses. The language of the bill is narrowly tailored so that an agency could only close an open session to discuss cybersecurity if such a discussion in an open meeting would prevent the agency from

effectively addressing the issue, implementing cybersecurity measures, or otherwise compromise the network security.

DOIT comments that information regarding the preparations against, or responses to, cyberattacks or cyber threats is sensitive in nature. For agencies that have boards or commission responsible for executive decisions of the agency, the ability to discuss and especially plan for cyber incidents is an important tool in combatting cyberattacks.

WHAT WILL BE THE CONSEQUENCES OF NOT ENACTING THIS BILL

Public bodies continue to be in an untenable position ensuring the duties and responsibilities assigned are secure and not compromised or exploited through cybersecurity incidents of which may be unrecoverable and irreversible.

JMA/jle/sb