Legislative Analysis

Phone: (517) 373-8080
http://www.house.mi.gov/hfa

Analysis available at
http://www.legislature.mi.gov

EXEMPT CERTAIN ELECTRONIC INFORMATION FROM FOIA

House Bill 4973 as enacted
Public Act 68 of 2018
Sponsor: Rep. Brandt Iden
House Committee: Communications and Technology
Senate Committee: Elections and Government Reform
Complete to 6-19-18

BRIEF SUMMARY: House Bill 4973 would amend the Freedom of Information Act (FOIA) to exempt certain electronic data related to cybersecurity measures from disclosure to the public.

FISCAL IMPACT: The bill would have no direct fiscal impact on the State or local governments. The bill could result in potential cost savings to the State and local governments if the exemption of the types of information specified in the bill were to indeed prevent a cybersecurity breach. As a general reference, the 2017 Ponemon Cost of Data Breach Study reports that the global average cost of a data breach is $3.6 million and the average cost for each lost or stolen record containing sensitive and confidential information is $141.

THE APPARENT PROBLEM:

While it is in an entity's best interest to work with authorities to combat cybersecurity incidents in order to protect private and sensitive data, private information could still be leaked to the public through certain FOIA requests. Currently, companies who suffer from a cybersecurity incident are wary of providing sensitive information to the police to help find and stop the perpetrator, as the shared information in the police report could be requested under FOIA. A representative from the Michigan State Police voiced this concern while testifying in support of House Bill 4973. He believes that the specific language this bill would provide is necessary to modernize FOIA and reflect the sensitive nature of certain company data so that an affected company would be more forthcoming with police and help to stop perpetrators of cybersecurity incidents.

THE CONTENT OF THE BILL:

Michigan's FOIA statute, Public Act 442 of 1976, establishes procedures and requirements for the disclosure of public records by all public bodies in the state. There are two classes of public records: those subject to disclosure and those exempt from disclosure. Generally, all records are subject to disclosure unless specifically exempted.

Currently, Section 13(1) of FOIA exempts from disclosure certain records. For instance, subdivision (y) exempts "records or information of measures designed to protect the security or safety of persons or property" from being disclosed to the public. The bill would amend this to add, "*or the confidentiality, integrity, or availability of information systems*."

The bill would further add that these systems could include, but are not limited to, ***cybersecurity plans, assessments, or vulnerabilities***.

> ***Cybersecurity plan*** would include, but not be limited to, information about a person's information systems, network security, encryption, network mapping, access control, passwords, authentication practices, computer hardware or software, or response to cybersecurity incidents.
>
> ***Cybersecurity assessment*** would mean an investigation undertaken by a person, governmental body, or other entity to identify vulnerabilities in cybersecurity plans.
>
> ***Cybersecurity vulnerability*** would mean a deficiency within computer hardware or software, or within a computer network or information system, that could be exploited by unauthorized parties for use against an individual computer user or a computer network or information system.

The bill also would amend Section 13(1) by adding the following subdivisions to provide the following exemptions from FOIA disclosure:

- (z) to exempt information that would identify or provide a means of identifying a person that may, as a result of disclosure, become a victim of a ***cybersecurity incident***. Information that would disclose a person's cybersecurity plans or other related practices, procedures, methods, results, organizational information system infrastructure, hardware, or software also would be exempt.
- (aa) to exempt research data on road and attendant infrastructure collected, measured, recorded, processes, or disseminated by a public agency or private entity, or information about software or hardware created or used by the private entity for such purposes.

Cybersecurity incident would include, but not be limited to:

- A computer network intrusion or attempted intrusion;
- A breach of primary computer network controls;
- Unauthorized access to programs, data, or information contained in a computer system;
- Or actions by a third party that materially affect component performance or, because of impact to component systems, prevent normal computer system activities.

The bill would also add to the definition of ***writing*** for purposes of the Act, to include hard drives and solid state storage components as means of recording or retaining meaningful content.

Finally, the bill would make stylistic and linguistic changes throughout FOIA to update references and clarify wording.

MCL 15.232 and 15.243

ARGUMENTS:

For:

Supporters of the bill argued that the new exemptions would help police in their investigations of cybersecurity incidents because companies would feel at ease that their sensitive data would stay secure and could not be requested under FOIA. If companies were able to help the police without the threat of having their sensitive and private information available under FOIA, then it would be easier for law enforcement to find perpetrators.

Against:

Concerns were raised with the bill regarding who would be able to decide what is proprietary to the company and if there would be a duty to notify the victims of the breach. The main premise was ensuring that information that would affect the public could still be available, such as knowing if your social security number has been stolen from a company database.

Response:

Supporters of the bill responded that the FOIA division within the Michigan State Police would be the ultimate decision maker regarding whether information is proprietary or not, and only when a FOIA request is made. The division would be responsible for determining which requested information falls under an exemption and which information is required to be disclosed. In addition, supporters of the bill feel that the bill and FOIA are designed to ensure that victims of a breach are notified.

Legislative Analyst: Emily S. Smith
Fiscal Analyst: Michael Cnossen