Senate Fiscal Agency
P. O. Box 30036
Lansing, Michigan 48909-7536

BILL ANALYSIS

Telephone: (517) 373-5383
Fax: (517) 373-1986

House Bill 4973 (as passed by the House)
Sponsor: Representative Brandt Iden
House Committee: Communications and Technology
Senate Committee: Elections and Government Reform

Date Completed: 2-20-18

CONTENT

The bill would amend the Freedom of Information Act (FOIA) to allow a public body to exempt the following from disclosure:

-- Records of measures designed to protect the confidentiality, integrity, or availability of certain information systems, as well as cybersecurity plans, assessments, or vulnerabilities.
-- Information that would reveal the identity of a person who could, as a result of disclosure of the information, become a victim of a cybersecurity incident, or that would reveal the person's cybersecurity plans, or cybersecurity-related practices.

Under the Act, upon providing a public body's FOIA coordinator with a written request that describes a public record sufficiently to enable the public body to find the public record, a person has a right to inspect, copy, or receive copies of the requested public record of the public body. The Act defines "public record" as a writing prepared, owned, used, in the possession of, or retained by a public body in the performance of an official function, form the time it is created.

A public body may exempt from disclosure records or information of measures designed to protect the security or safety of persons or property, whether public or private, including building, public works, and public water supply designs to the extent that those designs relate to the ongoing security measures of a public body, capabilities and plans for responding to a violation of the Michigan Anti-Terrorism Act, emergency response plans, risk planning documents, threat assessments, and domestic preparedness strategies, unless disclosure would not impair a public body's ability to protect the security or safety of persons or property or unless the public interest in disclosure outweighs the public interest in nondisclosure in the particular instance.

The bill also would allow the exemption of records or information of measures designed to protect the confidentiality, integrity, or availability of information systems, whether public or private, and cybersecurity plans, assessments, or vulnerabilities, unless disclosure would not impair a public body's ability to protect security or safety or unless the public interest in disclosure outweighed the public interest in nondisclosure. This exemption (including the current and proposed provisions) would not apply to information submitted as required by law or as a condition to receiving a governmental contract, license, or other benefit.

The bill also would allow a public body to exempt information that would identify or provide a means of identifying a person that could, as a result of disclosure of the information, become a victim of a cybersecurity incident, or that would disclose a person's cybersecurity plans or cybersecurity-related practices, procedures, methods, results, organizational information system infrastructure, hardware, or software. This exemption would not apply to information submitted as required by law or as a condition to receiving a governmental contract, license, or other benefit.

The bill would define "cybersecurity assessment" as an investigation undertaken by a person, governmental body, or other entity to identify vulnerabilities in cybersecurity plans.

"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.

"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 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 Act defines "writing" as handwriting, typewriting, printing, photostating, photographing, photocopying, and every other means of recording. The term includes letters, words, pictures, sounds, or symbols, or combinations of them, and papers, maps, magnetic or paper tapes, photographic films or prints, microfilm, microfiche, magnetic or punched cards, discs, drums, or other means of recording or retaining meaningful content. The bill also would include hard drives and solid state storage components.

The bill would take effect 90 days after it was enacted

MCL 15.232 & 15.243 Legislative Analyst: Nathan Leaman

FISCAL IMPACT

The bill would have no fiscal impact on State or local government.

Fiscal Analyst: Joe Carrasco

SAS\S1718\s4973sa