

FREEDOM OF INFORMATION EXCEPTIONS FOR CYBERSECURITY AND ENERGY INFRASTRUCTURE

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

House Bill 4540 (proposed substitute H-9)
Sponsor: Rep. Kurt Heise
First Committee: Oversight and Ethics
Second Committee: Natural Resources
Complete to 2-22-16

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

SUMMARY:

HB 4540 would amend Sections 2 and 13 of the Freedom of Information Act to allow a public body to exempt the following from disclosure:

- Cybersecurity plans, cybersecurity assessments, and cybersecurity threats.
- Information that would identify, or provide a means of identifying, a person that could, as a result of the disclosure, become a victim of a cybersecurity incident, or that would disclose a person's cybersecurity plans or practices, procedures, methods, results, organizational structure, hardware, or software.

The bill would take effect 90 days after the date it is enacted into law.

Key Terms

"Cybersecurity assessment" means an investigation undertaken by a person, governmental body, or other entity to identify vulnerabilities in cybersecurity plans.

"Cybersecurity incident" includes, but is not 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" includes, but is not limited to, information about a person's network security, encryption, network mapping, access control, passwords, authentication practices, computer hardware or software, or response to cybersecurity incidents.

"Cybersecurity vulnerability" means 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.

"Writing," which is presently defined in Section 2, would be amended by explicitly including hard drives and solid state storage components in the definition.

Added exemptions from FOIA

Section 13 contains exemptions as to the types of information that are not subject to disclosure under a FOIA request. Presently, an exemption exists for "records or information of measures designed to protect the security or safety of persons or property" both public and private.

The bill would amend this by adding that records and information relating to the "confidentiality, integrity, or availability of information systems" to this exemption and specifically stating that cybersecurity plans, assessments, and vulnerabilities are exempt. This provision also presently states these types of records and information are not exempt if 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.

Lastly, the bill would add an exemption for information that would "identify or provide a means of identifying a person that may, 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."

FISCAL IMPACT:

A fiscal analysis for the substitute is in process.

Legislative Analyst: Josh Roesner
Fiscal Analyst: Paul B.A. Holland

■ This analysis was prepared by nonpartisan House Fiscal Agency staff for use by House members in their deliberations, and does not constitute an official statement of legislative intent.