Legislative Analysis

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

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

FREEDOM OF INFORMATION EXCEPTIONS FOR CYBERSECURITY AND ENERGY INFRASTRUCTURE

House Bill 4540 as introduced
Sponsor: Rep. Kurt Heise
Committee: Oversight and Ethics
Complete to 5-13-15

SUMMARY:

The bill would amend 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.

- A record, document, or information that discloses critical energy infrastructure information.

"Critical energy infrastructure information" means specific engineering, vulnerability, or detailed design information about proposed or existing critical energy infrastructure that has all of the following characteristics: (1) relates details about the production, generation, transportation, transmission, or distribution of fuel or energy; (2) could be useful to a person in planning an attack on critical energy infrastructure; and (3) provides more than the general location of the critical infrastructure.

"Critical energy infrastructure" means existing and proposed systems and assets, whether physical or virtual, relating to crude oil, petroleum, electricity, or natural gas, the incapacity or destruction of which would negatively affect public security, economic security, health, safety, or any combination of those matters.

"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; 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, governmental body's, or other entity's network security, encryption, network mapping, access control, passwords, authentication practices, computer hardware or software, or response to cybersecurity incidents.

"Cybersecurity threat" means information about computer system vulnerabilities or planned exploitation of computer systems by unauthorized parties.

MCL 15.232 and 15.243

FISCAL IMPACT:

The bill would have no fiscal impact to state or local governments.

Legislative Analyst: Chris Couch
Fiscal Analyst: Perry Zielak

■ 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.