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 (Proposed H-6 substitute)
Sponsor: Rep. Kurt Heise
Committee: Oversight and Ethics
Complete to 12-10-15

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.

- Information that is presumed to be critical energy infrastructure information. A process for seeking such information is described below.

Critical Energy Infrastructure Information

Except as otherwise provided, a public body would have to exempt from disclosure information that is presumed to be critical energy infrastructure information. Information is presumed to be such information if, when submitted to a public body, the writing that includes the information prominently displays the designation "includes critical energy infrastructure information" and "do not disclose." The presumption continues until determined otherwise by the Michigan Agency for Energy (MAE).

When a person submits a writing containing such information to a public body, it would have to send the identical writing to the MAE, along with a copy of the identical writing with the critical energy infrastructure information redacted, as well as an explanation for the designation of the redacted information.

A public body (other than the MAE) would have to inform a person requesting such information that the information may be available from the MAE after the MAE has reviewed it to determine if it is critical energy infrastructure information.

If a public body denies a request for information, the person making the request could make a written request to the MAE information coordinator. The coordinator would notify the person who submitted the information and include a copy of the request. In making a determination about the information, the coordinator could consult with the Department of State Police, the Public Service Commission, the Department of Environmental Quality,

the Department of Technology, Management, and Budget, and the person who submitted the information.

If the coordinator finds that the information is critical energy infrastructure information, the request would be denied. If not, then the coordinator would disclose the information no later than 14 days after notifying the person who submitted the information. A person aggrieved by a determination of the MAE could file an appeal in the Court of Claims (within the Michigan Court of Appeals). That court would have exclusive jurisdiction.

Key Terms

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

"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.

FISCAL IMPACT:

The bill would have an indeterminate, yet likely nominal, fiscal impact on the Michigan Agency for Energy (MAE) to the extent that the MAE would incur administrative expenses to review FOIA requests pertaining to "critical energy infrastructure information" and potentially legal costs to defend its determinations. The bill would have an indeterminate, but likely nominal, fiscal impact on the Court of Claims, depending on how the bill affected caseloads and related administrative costs.

Legislative Analyst: Chris Couch
Fiscal Analyst: Paul B.A. Holland
Robin Risko