Legislative Analysis

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

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

CYBER CIVILIAN CORPS ACT

House Bill 4508 (reported from committee as H-1)
Sponsor: Rep. Brandt Iden
Committee: Communications and Technology
Complete to 6-10-17

BRIEF SUMMARY: House Bill 4508 would create the Cyber Civilian Corps Act to establish the Michigan Cyber Civilian Corps program within the Department of Technology, Management, and Budget (DTMB).

FISCAL IMPACT: The bill would have an indeterminate, but likely minimal, direct fiscal impact to the DTMB. The department is already an administrator to the existing Michigan Cyber Civilian Corps (MiC3) and would not incur significant costs to expand the program as described in the bill. There would likely be costs related to training an increased number of volunteers; however, these costs could be offset by charging clients a fee, an option the bill provides.

The bill could help reduce future negative fiscal impacts to local governments and state agencies. While additional volunteer workers would not replace any current full-time worker equivalent costs, an expanded volunteer program could help reduce costs to the state by mitigating the need for additional cybersecurity staff as cyber threats increase. The bill could also reduce potential future costs by minimizing the impact to government organizations and the disruption of services following a cybersecurity incident through the deployment of trained volunteers.

THE APPARENT PROBLEM:

The constant advancements in informational technology bring new cyber threats in tow. According to the bill sponsor, the State of Michigan detects tens of thousands cyberattacks every day. These threats are not only aimed at governments, though; businesses and nonprofits are also at risk for cyberattacks. Therefore, to protect government agencies and private entities in the state, a framework to provide for a team of trained individuals to help in times of disaster is crucial. Even though the Cyber Civilian Corps already exists, House Bill 4508 would put it into statute under the control of the Department of Technology, Management, and Budget.

THE CONTENT OF THE BILL:

House Bill 4508 would allow the DTMB to invite and appoint individuals to serve as Michigan Cyber Civilian Corps volunteers, and allow civilians with expertise in addressing cybersecurity incidents to volunteer and provide a rapid response and assistance to a municipal, educational, nonprofit, or business organization in need of expert assistance during a "cybersecurity incident."

"Cybersecurity incident" refers to an event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident on any of these. A cybersecurity incident includes, but is not limited to, the existence of a vulnerability in an information system, system security procedures, internal controls, or implementation that is subject to exploitation.

The department could provide appropriate training to prospective and existing volunteers, and could provide compensation for actual and necessary travel and subsistence expenses incurred by Michigan cyber civilian corps volunteers on a deployment at the discretion of the department.

Michigan Cyber Civilian Corps volunteer

A "Michigan Cyber Civilian Corps volunteer" refers to an individual who has entered into a volunteer agreement with the DTMB to serve as a volunteer in the corps. The department would enter into such a volunteer contract with any individual who wishes to accept an invitation to serve as a volunteer. At a minimum, the contract would have to include all of the following provisions:

- Acknowledging the confidentiality of information relating to this state, state residents, and clients. (Client refers to a municipal, educational, nonprofit, or business organization that has requested and is using the rapid response assistance of the civilian corps under the direction of the department.)
- Protecting from disclosure any confidential information of this state, state residents, or clients acquired by the volunteer through participation in the program.
- Requiring the volunteer to avoid conflicts of interest that might arise from a particular deployment; comply with all existing DTMB security policies and procedures regarding information technology resources; consent to background screening considered appropriate by the department under this act; and attest that he or she meets any standards of expertise that may be established by the department.

A Michigan Cyber Civilian Corps volunteer would not be classified as an agent, employee, or independent contractor of this state for any purpose and would have no authority to bind this state with regard to third parties. This state would also not be liable to a volunteer for personal injury or property damage suffered by volunteer through participation in the corps program.

Background check

When an individual accepts an invitation to serve as a volunteer, the department must request the Department of State Police to conduct a criminal records check through the Federal Bureau of Investigation and a criminal history check on the individual. The department shall make the request on a form and in the manner prescribed by the department of state police. The volunteer must give written consent, and submit fingerprints. The MSP must report results within a reasonable time and provide the results

of the criminal records check from the FBI. The MSP may also charge the DTMB a fee for a criminal history check or a criminal records check that does not exceed the actual and reasonable cost of conducting the check.

Immunity from civil liability

Except as otherwise provided in the act, the DTMB and this state would be immune from tort liability for acts or omissions by a volunteer. In addition, also except as otherwise provided in the act, and without regard to discretionary or ministerial nature of the conduct of a volunteer, each volunteer would be immune from tort liability for an injury to a person or damage to property that occurred while deployed and acting on behalf of the DTMB, but only if all of the following are met:

- The volunteer is acting or reasonably believes that he or she is acting within the scope of his or her authority.
- The volunteer's conduct does not amount to gross negligence that is the proximate cause of the injury or damage. Gross negligence would mean conduct that is so reckless that it demonstrates a substantial lack of concern for whether an injury would occur.
- The volunteer's conduct is not a material breach of the volunteer agreement during that deployment.

If a claim is made or a civil or criminal action is commenced against a volunteer, and the above requirements are met, the DTMB could pay for, engage, or furnish the services of an attorney to advise the volunteer as to the claim and to appear for and represent the volunteer in the action. The DTMB could also compromise, settle, and pay a civil claim before or after the commencement of a civil action or for a judgment for damages, as well as indemnify the volunteer for a judgment. Furthermore, a volunteer could obtain reimbursement for legal expenses incurred stemming from a criminal action.

Deployment

On the occurrence of a cybersecurity incident that affects a client, the client may request DTMB to deploy one or more volunteers to provide rapid response assistance under the direction of the department. The department would have discretion to initiate deployment of volunteers upon the occurrence of a cybersecurity incident and the request of a client. The deployment of a volunteer to assist a client would be for seven days, unless the writing initiating the deployment contains a different period. At the direction of the department, the deployment of a volunteer could be extended in writing in the same manner as the initial deployment.

A volunteer would be able to decline to accept deployment for any reason. If a volunteer accepts deployment for a cybersecurity incident, acceptance would have be in writing.

To initiate the deployment of a volunteer for a cybersecurity incident, the department would indicate in writing that the volunteer is authorized to provide the assistance. A single writing could initiate the deployment of more than one volunteer. The department would also be required to maintain the writing for six years from the time of deployment or for the time required under the department's record retention policies, whichever is longer.

Advisory board

The Michigan Cyber Civilian Corps Advisory Board would be created as an advisory body within the department. The advisory board would be composed of the Adjutant General (National Guard), the director DTMB, the director of Michigan State Police, and the director of the Department of Talent and Economic Development (or their designees). The advisory board would also be responsible in reviewing and making recommendations to the STMB regarding the policies and procedures to be used in implementing this act.

Department responsibilities

After consultation with the advisory board, the DTMB's chief information officer would be required to approve the set of tools that the corps could use in response to a cybersecurity incident and to determine the standards of expertise necessary for an individual to become a member of the corps. (The "chief information officer" is defined in the bill the individual within the DTMB designated by the governor as the chief information officer for the state.)

Also after consultation with the advisory board, the department would be required to publish guidelines for the operation of the corps program. At a minimum, the published guidelines would have to include the following:

- An explanation of the standard use to determine whether an individual could serve as a volunteer and an explanation of the process by which an individual could become a volunteer.
- An explanation of the requirements imposed for a client to receive the assistance of the corps and an explanation of the process by which a client may request and receive assistance.

The DTMB would be the entity to enter into contracts with clients as a condition to providing assistance through the corps. The department could also establish a fee schedule for clients. The department may recoup expenses through the fees but may not generate a profit.

This act would take effect 90 days after the date it is enacted into law.

BACKGROUND INFORMATION:

The Michigan Cyber Civilian Corps (MiC3) is a group of trained cybersecurity experts who volunteer to provide expert assistance to enhance the state's ability to rapidly resolve cyber incidents when activated under a Governor declared State of Emergency. The group includes 52 volunteers from government, education, and business sectors, and they hope to raise membership to 200 volunteers.

The mission of MiC3 is to work with government, education, private sector organizations, and volunteers to create and implement a rapid response team to be activated under a Governor declared cyber State of Emergency and to provide mutual aid to government, education, and business organizations in the State of Michigan.

Membership is currently open to information security professionals who are residents of the state of Michigan. According to their website, applicants should have at least two years of direct involvement with information security, preferably security operations, incident response and/or digital or network forensics. Applicants should also have a basic security certification (ANSI-certified/DOD 8570 compliant certifications such as Security+, C|EH, CISSP, or GIAC certifications are strongly preferred). Applicants will also be required to pass a series of tests to demonstrate basic knowledge of networking and security concepts, as well as basic IR and forensics skills. Because of the time commitment (up to 10 days/year for training and exercises), applicants must provide evidence of employer support. Successful applicants will also be subject to background screening and sign a confidential disclosure agreement.[1]

ARGUMENTS:

For:

Proponents of the bill believe that with the rapid development of information technology and constant reliance on its functioning, Michigan and businesses within the state are at an ever-increasing risk of disastrous outcomes in the event of a cyber attack. The program created under the bill and headed by the DTMB would ensure that the state and various business could bounce back quickly if a cyber incident occurs.

Against:

Opponents of the bill are concerned that a state-run volunteer program for specialized technological services would hinder the private sector. The bill appears to be anti-competitive in nature as local businesses would be shut out of business opportunities: if someone can get the same services for free through the volunteer program, why would they pay a private company?

Response:

Supporters of the bill have responded to this concern by stating that the program is meant to aid with very large-scale or disaster-type cyber incidents. Volunteers under the program would not be deployed for everyday incidents (such as simple hacking); there will still be a market for private businesses for other incidents.

POSITIONS:

A representative from the following entities testified in support of the bill on 5-9-17:

- Michigan Bankers Association
- Michigan Department of Military and Veterans Affairs
- Michigan Department of Technology, Management, and Budget
- Michigan Financial Industry Cybersecurity Council

Representatives from the following entities indicated support for the bill on 5-9-17 or 5-23-17:

[1] State of Michigan, Michigan Cyber Civilian Corps,http://www.michigan.gov/som/0,4669,7-192-78403_78404_78419---,00.html, 2017.

- AT&T
- Michigan State Police
- National Guard Association
- Michigan Chamber of Commerce
- Community Bankers of Michigan
- Small Business Association of Michigan

A representative from SEQURIS Group, LLC testified in opposition to the bill on 5-9-17.

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

■ 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.