CYBER CIVILIAN CORPS ACT
Act 132 of 2017

AN ACT to create a program under which volunteers may provide services to organizations in this state to respond to cybersecurity incidents; to provide for protection from liability for personal injury and property damage; to provide for the powers and duties of state governmental officers and agencies; and to create the Michigan cyber civilian corps advisory board and prescribe its powers and duties.

History: 2017, Act 132, Eff. Jan. 24, 2018.

The People of the State of Michigan enact:

18.221 Short title.

Sec. 1. This act shall be known and may be cited as the "cyber civilian corps act".

History: 2017, Act 132, Eff. Jan. 24, 2018.

18.222 Definitions.

Sec. 2. As used in this act:

(a) "Advisory board" means the Michigan cyber civilian corps advisory board created under section 9.

(b) "Chief information officer" means the individual within the department designated by the governor as the chief information officer for this state.

(c) "Client" means a municipal, educational, nonprofit, or business organization that has requested and is using the rapid response assistance of the Michigan cyber civilian corps under the direction of the department.

(d) "Cybersecurity incident" means 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. 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.

(e) "Department" means the department of technology, management, and budget.

(f) "Michigan cyber civilian corps" means the program established by this act under which civilian volunteers who have expertise in addressing cybersecurity incidents may volunteer at the invitation of the department to provide rapid response assistance to a municipal, educational, nonprofit, or business organization in need of expert assistance during a cybersecurity incident.

(g) "Michigan cyber civilian corps volunteer" means an individual who has entered into a volunteer agreement with the department to serve as a volunteer in the Michigan cyber civilian corps.

(h) "Volunteer agreement" means the contract entered into between the department and a Michigan cyber civilian corps volunteer under section 4.

History: 2017, Act 132, Eff. Jan. 24, 2018.

18.223 Michigan cyber civilian corps volunteers; appointment; purpose.

Sec. 3. The department may appoint individuals to serve as Michigan cyber civilian corps volunteers for the purposes of facilitating the responsibilities of the department as provided in this act.

History: 2017, Act 132, Eff. Jan. 24, 2018.

18.224 Service as Michigan cyber civilian corps volunteer; contract.

Sec. 4. The department shall enter into a contract with any individual who wishes to accept an invitation by the department to serve as a Michigan cyber civilian corps volunteer. The contract must include, at a minimum, all of the following:

(a) A provision acknowledging the confidentiality of information relating to this state, state residents, and clients.

(b) A provision protecting from disclosure any confidential information of this state, state residents, or clients acquired by the Michigan cyber civilian corps volunteer through participation in the Michigan cyber civilian corps.

(c) A provision requiring the Michigan cyber civilian corps volunteer to avoid conflicts of interest that might arise from a particular deployment.

(d) A provision requiring the Michigan cyber civilian corps volunteer to comply with all existing department security policies and procedures regarding information technology resources.

(e) A provision requiring the Michigan cyber civilian corps volunteer to consent to background screening

considered appropriate by the department under this act, and a section in which the individual gives that consent as described in section 5.

(f) A provision requiring the Michigan cyber civilian corps volunteer to attest that he or she meets any standards of expertise that may be established by the department.

History: 2017, Act 132, Eff. Jan. 24, 2018.

18.225 Criminal history check and criminal records check.

Sec. 5. (1) When an individual accepts an invitation to serve as a Michigan cyber civilian corps volunteer as described in section 4, the department shall request the department of state police to do both of the following:

(a) Conduct a criminal history check on the individual.

(b) Conduct a criminal records check through the Federal Bureau of Investigation on the individual.

(2) An individual who accepts an invitation to the Michigan cyber civilian corps shall give written consent in the volunteer agreement for the department of state police to conduct the criminal history check and criminal records check required under this section. The department shall require the individual to submit his or her fingerprints to the department of state police and the Federal Bureau of Investigation for the criminal records check.

(3) The department shall request a criminal history check and criminal records check under this section on all individuals who wish to participate as Michigan cyber civilian corps volunteers. The department shall make the request on a form and in the manner prescribed by the department of state police.

(4) Within a reasonable time after receiving a complete request by the department for a criminal history check and criminal records check on an individual under this section, the department of state police shall conduct the criminal history check and provide a report of the results to the department. The report must indicate that the individual is cleared or not cleared to become a Michigan cyber civilian corps volunteer.

(5) Within a reasonable time after receiving a proper request by the department for a criminal records check on an individual under this section, the department of state police shall initiate the criminal records check with the Federal Bureau of Investigation. After receiving the results of the criminal records check from the Federal Bureau of Investigation, the department of state police shall provide a report to the department that indicates that the individual is cleared or not cleared to become a Michigan cyber civilian corps volunteer.

(6) If a criminal arrest fingerprint is subsequently submitted to the department of state police and matches against a fingerprint that was submitted pursuant to this act and stored in its automated fingerprint identification system (AFIS) database, the department of state police shall notify the department that the individual is still cleared or is no longer cleared to continue as a Michigan cyber civilian corps volunteer. When the department of state police is able to participate with the Federal Bureau of Investigation automatic notification system, then any subsequent arrest fingerprint submitted to the Federal Bureau of Investigation must also be reviewed by the department of state police. The department of state police shall provide a report to the department that indicates that the individual is still cleared or is no longer cleared to continue as a Michigan cyber civilian corps volunteer.

History: 2017, Act 132, Eff. Jan. 24, 2018.

18.226 Michigan cyber civilian corps volunteer as agent, employee, or independent contractor; liability of state.

Sec. 6. (1) A Michigan cyber civilian corps volunteer is not an agent, employee, or independent contractor of this state for any purpose and has no authority to bind this state with regard to third parties.

(2) This state is not liable to a Michigan cyber civilian corps volunteer for personal injury or property damage suffered by the Michigan cyber civilian corps volunteer through participation in the Michigan cyber civilian corps.

History: 2017, Act 132, Eff. Jan. 24, 2018.

18.227 Immunity from tort liability; conditions; compromise, settlement, or payment of claim by department; reimbursement for legal expenses; "gross negligence" defined.

Sec. 7. (1) Except as otherwise provided in this section, the department and this state are immune from tort liability for acts or omissions by a Michigan cyber civilian corps volunteer under this act.

(2) Except as otherwise provided in this section, and without regard to discretionary or ministerial nature of the conduct of a Michigan cyber civilian corps volunteer, each Michigan cyber civilian corps volunteer is immune from tort liability for an injury to a person or damage to property that occurred while deployed and acting on behalf of the department if all of the following are met:

(a) The Michigan cyber civilian corps volunteer is acting or reasonably believes that he or she is acting within the scope of his or her authority.

(b) The Michigan cyber civilian corps volunteer's conduct does not amount to gross negligence that is the proximate cause of the injury or damage.

(c) The Michigan cyber civilian corps volunteer's conduct is not a material breach of the volunteer agreement during that deployment.

(3) If a claim is made or a civil action is commenced against a Michigan cyber civilian corps volunteer for injuries to persons or property caused by negligence of a Michigan cyber civilian corps volunteer that occurred while in the course of his or her deployment on behalf of the department and while acting within the scope of his or her authority, the department may pay for, engage, or furnish the services of an attorney to advise the Michigan cyber civilian corps volunteer as to the claim and to appear for and represent the Michigan cyber civilian corps volunteer in the action. The department may compromise, settle, and pay the claim before or after the commencement of a civil action. Whenever a judgment for damages is awarded against a Michigan cyber civilian corps volunteer as a result of a civil action for personal injuries or property damage caused by the Michigan cyber civilian corps volunteer while in the course of his or her deployment and while acting within the scope of his or her authority, the department may indemnify the Michigan cyber civilian corps volunteer or pay, settle, or compromise the judgment.

(4) If a criminal action is commenced against a Michigan cyber civilian corps volunteer based upon the conduct of the Michigan cyber civilian corps volunteer in the course of his or her deployment, if the Michigan cyber civilian corps volunteer had a reasonable basis for believing that he or she was acting within the scope of his or her authority at the time of the alleged conduct, the department may pay for, engage, or furnish the services of an attorney to advise the Michigan cyber civilian corps volunteer as to the action, and to appear for and represent the Michigan cyber civilian corps volunteer in the action. A Michigan cyber civilian corps volunteer who has incurred legal expenses for conduct prescribed in this subsection may obtain reimbursement for those expenses under this subsection.

(5) This section does not impose liability on this state or the department.

(6) As used in this section, "gross negligence" means conduct so reckless as to demonstrate a substantial lack of concern for whether an injury results.

History: 2017, Act 132, Eff. Jan. 24, 2018.

18.228 Deployment of Michigan cyber civilian corps volunteers.

Sec. 8. (1) On the occurrence of a cybersecurity incident that affects a client, the client may request the department to deploy 1 or more Michigan cyber civilian corps volunteers to provide rapid response assistance under the direction of the department.

(2) The department, in its discretion, may initiate deployment of Michigan cyber civilian corps volunteers upon the occurrence of a cybersecurity incident and the request of a client.

(3) Acceptance of a deployment by a Michigan cyber civilian corps volunteer for a particular cybersecurity incident must be made in writing. A Michigan cyber civilian corps volunteer may decline to accept deployment for any reason.

(4) To initiate the deployment of a Michigan cyber civilian corps volunteer for a particular cybersecurity incident, the department shall indicate in writing that the Michigan cyber civilian corps volunteer is authorized to provide the assistance. A single writing may initiate the deployment of more than 1 Michigan cyber civilian corps volunteer.

(5) The department shall maintain a writing initiating the deployment of a Michigan cyber civilian corps volunteer to provide assistance to a client for 6 years from the time of deployment or for the time required under the department's record retention policies, whichever is longer.

(6) The deployment of a Michigan cyber civilian corps volunteer to provide assistance to a client must be for 7 days unless the writing initiating the deployment contains a different period.

(7) At the direction of the department, the deployment of a Michigan cyber civilian corps volunteer may be extended in writing in the same manner as the initial deployment.

History: 2017, Act 132, Eff. Jan. 24, 2018.

18.229 Michigan cyber civilian corps advisory board; creation; composition; duties.

Sec. 9. (1) The Michigan cyber civilian corps advisory board is created as an advisory body within the department.

(2) The Michigan cyber civilian corps advisory board is composed of the adjutant general, the director of the department, the director of the department of state police, and the director of the department of talent and economic development or their designees.

(3) The Michigan cyber civilian corps advisory board shall review and make recommendations to the department regarding the policies and procedures used by the department in implementing this act.

History: 2017, Act 132, Eff. Jan. 24, 2018.

18.230 Chief information officer; duties; operation guidelines; contracts with clients; training; compensation for travel and expenses; fee schedule; disclosure of information.

Sec. 10. (1) After consultation with the advisory board, the chief information officer shall do both of the following:

(a) Approve the set of tools that the Michigan cyber civilian corps may use in response to a cybersecurity incident.

(b) Determine the standards of expertise necessary for an individual to become a member of the Michigan cyber civilian corps.

(2) After consultation with the advisory board, the department shall publish guidelines for the operation of the Michigan cyber civilian corps program. At a minimum, the published guidelines must include the following:

(a) An explanation of the standard the department will use to determine whether an individual may serve as a Michigan cyber civilian corps volunteer and an explanation of the process by which an individual may become a Michigan cyber civilian corps volunteer.

(b) An explanation of the requirements the department will impose for a client to receive the assistance of the Michigan cyber civilian corps and an explanation of the process by which a client may request and receive the assistance of the Michigan cyber civilian corps.

(3) The department may enter into contracts with clients as a condition to providing assistance through the Michigan cyber civilian corps.

(4) The department may provide appropriate training to individuals who wish to participate in the Michigan cyber civilian corps and to existing Michigan cyber civilian corps volunteers.

(5) The department may 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.

(6) The department may establish a fee schedule for clients that wish to use the assistance of the Michigan cyber civilian corps. The department may recoup expenses through the fees but may not generate a profit.

(7) Information voluntarily given to the Michigan cyber command center or obtained under this act 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 is exempt from disclosure under the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246.

History: 2017, Act 132, Eff. Jan. 24, 2018.