16E.36 CYBERSECURITY INCIDENTS.

Subdivision 1. **Definitions.** (a) For purposes of this section, the following terms have the meanings given.

(b) "Bureau" means the Bureau of Criminal Apprehension.

(c) "Cybersecurity incident" means an action taken through the use of an information system or network that results in an actual or potentially adverse effect on an information system, network, or the information residing therein.

(d) "Cyber threat indicator" means information that is necessary to describe or identify:

(1) malicious reconnaissance, including but not limited to anomalous patterns of communication that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or vulnerability;

(2) a method of defeating a security control or exploitation of a security vulnerability;

(3) a security vulnerability, including but not limited to anomalous activity that appears to indicate the existence of a security vulnerability;

(4) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;

(5) malicious cyber command and control;

(6) the actual or potential harm caused by an incident, including but not limited to a description of the data exfiltrated as a result of a particular cyber threat; and

(7) any other attribute of a cyber threat, if disclosure of such attribute is not otherwise prohibited by law.

(e) "Defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cyber threat or security vulnerability, but does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting an information system not owned by the entity operating the measure, or another entity that is authorized to provide consent and has provided consent to that private entity for operation of the measure.

(f) "Government contractor" means an individual or entity that performs work for or on behalf of a public agency on a contract basis with access to or hosting of the public agency's network, systems, applications, or information.

(g) "Information resource" means information and related resources, such as personnel, equipment, funds, and information technology.

(h) "Information system" means a discrete set of information resources organized for collecting, processing, maintaining, using, sharing, disseminating, or disposing of information.

(i) "Information technology" means any equipment or interconnected system or subsystem of equipment that is used in automatic acquisition, storage, manipulation, management, movement, control, display,

switching, interchange, transmission, or reception of data or information used by a public agency or a government contractor under contract with a public agency which requires the use of the equipment or requires the use, to a significant extent, of the equipment in the performance of a service or the furnishing of a product. The term information technology also has the meaning given to information and telecommunications technology systems and services in section 16E.03, subdivision 1, paragraph (b).

(j) "Private entity" means any individual, corporation, company, partnership, firm, association, or other entity, but does not include a public agency, or a foreign government, or any component thereof.

(k) "Public agency" means any public agency of the state or any political subdivision; school districts; charter schools; intermediate districts; cooperative units under section 123A.24, subdivision 2; and public postsecondary education institutions.

(l) "Superintendent" means the superintendent of the Bureau of Criminal Apprehension.

Subd. 2. **Report on cybersecurity incidents.** (a) Beginning December 1, 2024, the head of or the decision-making body for a public agency must report a cybersecurity incident that impacts the public agency to the commissioner. A government contractor or vendor that provides goods or services to a public agency must report a cybersecurity incident to the public agency if the incident impacts the public agency.

(b) The report must be made within 72 hours of when the public agency or government contractor reasonably identifies or believes that a cybersecurity incident has occurred.

(c) The commissioner must coordinate with the superintendent to promptly share reported cybersecurity incidents.

(d) By September 30, 2024, the commissioner, in coordination with the superintendent, must establish a cyber incident reporting system having capabilities to facilitate submission of timely, secure, and confidential cybersecurity incident notifications from public agencies, government contractors, and private entities to the office.

(e) By September 30, 2024, the commissioner must develop, in coordination with the superintendent, and prominently post instructions for submitting cybersecurity incident reports on the department and bureau websites. The instructions must include, at a minimum, the types of cybersecurity incidents to be reported and a list of other information to be included in a report made through the cyber incident reporting system.

(f) The cyber incident reporting system must permit the commissioner, in coordination with the superintendent, to:

(1) securely accept a cybersecurity incident notification from any individual or private entity, regardless of whether the entity is a public agency or government contractor;

(2) track and identify trends in cybersecurity incidents reported through the cyber incident reporting system; and

(3) produce reports on the types of incidents, cyber threat, indicators, defensive measures, and entities reported through the cyber incident reporting system.

(g) Any cybersecurity incident report submitted to the commissioner is security information pursuant to section 13.37, is not discoverable in a civil or criminal action absent a court order or a search warrant, and is not subject to subpoena.

(h) Notwithstanding the provisions of paragraph (g), the commissioner may anonymize and share cyber threat indicators and relevant defensive measures to help prevent attacks and share cybersecurity incident notifications with potentially impacted parties through cybersecurity threat bulletins or relevant law enforcement authorities.

(i) Information submitted to the commissioner through the cyber incident reporting system is subject to privacy and protection procedures developed and implemented by the office, which shall be based on the comparable privacy protection procedures developed for information received and shared pursuant to the federal Cybersecurity Information Sharing Act of 2015, United States Code, title 6, section 1501, et seq.

Subd. 3. **Annual report to the governor and legislature.** Beginning January 31, 2026, and annually thereafter, the commissioner, in coordination with the superintendent, must submit a report on its cyber security incident report collection and resolution activities to the governor and to the legislative commission on cybersecurity. The report must include, at a minimum:

(1) information on the number of notifications received and a description of the cybersecurity incident types during the one-year period preceding the publication of the report;

(2) the categories of reporting entities that submitted cybersecurity reports; and

(3) any other information required in the submission of a cybersecurity incident report, noting any changes from the report published in the previous year.

History: *2024 c 123 art 17 s 24*