SENATE
STATE OF MINNESOTA
NINETY-THIRD SESSION

S.F. No. 4874

(SENATE AUTHORS: WIKLUND)

DATE	D-PG	OFFICIAL STATUS
03/13/2024	12183	Introduction and first reading Referred to State and Local Government and Veterans

A bill for an act

relating to cybersecurity; requiring reporting of cybersecurity incidents impacting public-sector organizations in Minnesota; proposing coding for new law in Minnesota Statutes, chapter 16E.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF MINNESOTA:

Section 1. **[16E.36] CYBERSECURITY INCIDENTS.**

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

(b) "Cybersecurity incident" means actions taken through the use of an information system or network that result in an actual or potentially adverse effect on an information system, network, and the information residing therein.

(c) "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.

(d) "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 such 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 such measure.

(e) "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.

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

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

(h) "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 such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product.

The term information technology also has the meaning described to information and telecommunications technology systems and services in section 16E.03, subdivision 1, paragraph (b).

(i) "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.

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

Subd. 2. **Report on cybersecurity incidents to the Bureau of Criminal Apprehension.** (a) Beginning December 1, 2024, cybersecurity incidents that impact state agencies; political subdivisions; school districts, charter schools, intermediate districts, cooperative units and public postsecondary education institutions shall report cybersecurity incidents to the Bureau of Criminal Apprehension in coordination with the Department of Information Technology Services. Cybersecurity incidents that impact third-party vendors and contractors utilized by reporting entities must also be reported.

(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) By September 30, 2024, the Superintendent of the Bureau of Criminal Apprehension in coordination with the Department of Information Technology Services shall establish cyber incident reporting capabilities to facilitate submission of timely, secure, and confidential cybersecurity incident notifications from public agencies, government contractors, and private entities to the office.

(d) By September 30, 2024, the Superintendent of the Bureau of Criminal Apprehension shall prominently post instructions for submitting cybersecurity incident notifications on its website. The instructions shall include, at a minimum, the types of cybersecurity incidents to be reported and any other information to be included in the notifications made through the established cyber incident reporting system.

(e) The cyber incident reporting system shall permit the Bureau of Criminal Apprehension in coordination with the Department of Information Technology Services 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, indicators, defensive measures, and entities reported through the cyber incident reporting system.

(f) Any cybersecurity incident notification submitted to the Bureau of Criminal Apprehension is security information pursuant to section 13.37 and is not discoverable in a civil or criminal action absent a court or a search warrant, and is not subject to subpoena.

(g) Notwithstanding the provisions of paragraph (f), the Bureau of Criminal Apprehension may anonymize and share cyber threat indicators and relevant defensive measures to help prevent additional or future attacks and share cybersecurity incident notifications with relevant law enforcement authorities.

(h) Information submitted to the Bureau of Criminal Apprehension through the cyber incident reporting system shall be 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, or the next business day following and annually thereafter, the Bureau of Criminal Apprehension in coordination with the Department of Information Technology Services shall submit an annual report on its activities to the governor and to the legislative commission on cybersecurity. The report shall 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 notifications; and

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

EFFECTIVE DATE. This section is effective November 30, 2024.