554G.3 Cybersecurity program framework.

1. A covered entity's cybersecurity program, as described in section 554G.2, reasonably conforms to an industry-recognized cybersecurity framework for purposes of section 554G.2 if any of the following are true:

a. (1) The cybersecurity program reasonably conforms to the current version of any of the following or any combination of the following, subject to subparagraph (2) and subsection 2:

(a) The framework for improving critical infrastructure cybersecurity developed by the national institute of standards and technology.

(b) National institute of standards and technology special publication 800-171.

(c) National institute of standards and technology special publications 800-53 and 800-53a.

(d) The federal risk and authorization management program security assessment framework.

(e) The center for internet security critical security controls for effective cyber defense.

(f) The international organization for standardization/international electrotechnical commission 27000 family — information security management systems.

(2) When a final revision to a framework listed in subparagraph (1) is published, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform the elements of its cybersecurity program to the revised framework within the time frame provided in the relevant framework upon which the covered entity intends to rely to support its affirmative defense, but in no event later than one year after the publication date stated in the revision.

b. (1) The covered entity is regulated by the state, by the federal government, or both, or is otherwise subject to the requirements of any of the laws or regulations listed below, and the cybersecurity program reasonably conforms to the entirety of the current version of any of the following, subject to subparagraph (2):

(a) The security requirements of the federal Health Insurance Portability and Accountability Act of 1996, as set forth in 45 C.F.R. pt. 164, subpt. C.

(b) Title V of the federal Gramm-Leach-Bliley Act of 1999, Pub. L. No. 106-102, as amended.

(c) The federal Information Security Modernization Act of 2014, Pub. L. No. 113-283.

(d) The federal Health Information Technology for Economic and Clinical Health Act as set forth in 45 C.F.R. pt. 162.

(e) Chapter 507F.

(f) Any applicable rules, regulations, or guidelines for critical infrastructure protection adopted by the federal environmental protection agency, the federal cybersecurity and infrastructure security agency, or the north American reliability corporation.

(2) When a framework listed in subparagraph (1) is amended, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform the elements of its cybersecurity program to the amended framework within the time frame provided in the relevant framework upon which the covered entity intends to rely to support its affirmative defense, but in no event later than one year after the effective date of the amended framework.

c. (1) The cybersecurity program reasonably complies with both the current version of the payment card industry data security standard and conforms to the current version of another applicable industry-recognized cybersecurity framework listed in paragraph "*a*", subject to subparagraph (2) and subsection 2.

(2) When a final revision to the payment card industry data security standard is published, a covered entity whose cybersecurity program reasonably complies with that standard shall reasonably comply the elements of its cybersecurity program with the revised standard within the time frame provided in the relevant framework upon which the covered entity intends to rely to support its affirmative defense, but not later than the effective date for compliance.

2. If a covered entity's cybersecurity program reasonably conforms to a combination of industry-recognized cybersecurity frameworks, or complies with a standard, as in the case of the payment card industry data security standard, as described in subsection 1,

paragraph *"a"* or *"c"*, and two or more of those frameworks are revised, the covered entity whose cybersecurity program reasonably conforms to or complies with, as applicable, those frameworks shall reasonably conform the elements of its cybersecurity program to or comply with, as applicable, all of the revised frameworks within the time frames provided in the relevant frameworks but in no event later than one year after the latest publication date stated in the revisions.

2023 Acts, ch 63, §3
Referred to in §554G.2