Ohio Revised Code

Section 1354.03 Reasonable conformance.

Effective: November 2, 2018
Legislation: Senate Bill 220 - 132nd General Assembly

A covered entity's cybersecurity program, as described in section 1354.02 of the Revised Code, reasonably conforms to an industry recognized cybersecurity framework for purposes of that section if division (A), (B), or (C) of this section is satisfied.

(A)(1) The cybersecurity program reasonably conforms to the current version of any of the following or any combination of the following, subject to divisions (A)(2) and (D) of this section:

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

(b) "NIST special publication 800-171";

(c) "NIST special publications 800-53 and 800-53a";

(d) The "federal risk and authorization management program (FedRAMP) 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 division (A)(1) of this section is published, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform to the revised framework not 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 division (B)(2) of this section:

(a) The security requirements of the "Health Insurance Portability and Accountability Act of 1996," as set forth in 45 CFR Part 164 Subpart C;

(b) Title V of the "Gramm-Leach-Bliley Act of 1999," Public Law 106-102, as amended;

(c) The "Federal Information Security Modernization Act of 2014," Public Law 113-283;

(d) The "Health Information Technology for Economic and Clinical Health Act," as set forth in 45 CFR part 162.

(2) When a framework listed in division (B)(1) of this section is amended, a covered entity whose cybersecurity program reasonably conforms to that framework shall reasonably conform to the amended framework not 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 (PCI) data security standard" and conforms to the current version of another applicable industry recognized cybersecurity framework listed in division (A) of this section, subject to divisions (C)(2) and (D) of this section.

(2) When a final revision to the "PCI data security standard" is published, a covered entity whose cybersecurity program reasonably complies with that standard shall reasonably comply with the revised standard not later than one year after the publication date stated in the revision.

(D) 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 (PCI) data security standard, as described in division (A) or (C) of this section, 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 to or comply with, as applicable, all of the revised frameworks not later than one year after the latest

publication date stated in the revisions.