OHIO LEGISLATIVE SERVICE COMMISSION

Sub. Bill Comparative Synopsis

Emily E. Wendel

S.B. 220

132nd General Assembly
(S. Gov't Oversight & Reform)

This table summarizes how the latest substitute version of the bill differs from the immediately preceding version. It addresses only the topics on which the two versions differ substantively. It does not list topics on which the two bills are substantively the same.

Topic	Previous Version (As Introduced)	Sub. Version (L_132_0943-5)
Covered entities	Specifies that a covered entity for purposes of the bill is a business that accesses, maintains, communicates, or handles personal information. Defines "business" as any limited liability company, limited liability partnership, corporation, sole proprietorship, or nonprofit corporation or unincorporated nonprofit association that operates in Ohio *(R.C. 1354.01(A) and (B))*.	Specifies that a covered entity for purposes of the bill is a business that accesses, maintains, communicates, or processes personal information in or through one or more systems, networks, or services located in or outside Ohio. Defines "system" to have the same meaning as in the Consumer Protection Law. Defines "business" as any limited liability company, limited liability partnership, corporation, sole proprietorship, association, or other group, however organized and whether operating for profit or not for profit, including a financial institution organized, chartered, or holding a license authorizing operation under the laws of Ohio, any other state, the United States, or any other country, or the parent or subsidiary

Topic	Previous Version (As Introduced)	Sub. Version (L_132_0943-5)
		of a financial institution *(R.C. 1354.01(A), (B), and (D))*.
Affirmative defense	Requires a covered entity seeking a safe harbor under the bill to create, maintain, and comply with a written cybersecurity program that meets the bill's requirements, including requirements regarding the features, scale, and scope of the program and a requirement that the program comply with an industry cybersecurity framework listed in the bill. States that a covered entity that implements and maintains a cybersecurity program that complies with an industry cybersecurity framework listed in the bill must be deemed to be in compliance with the section of law that creates the affirmative defense. States that compliance with that section constitutes an affirmative defense to any cause of action sounding in tort that alleges the failure to implement reasonable security controls resulted in a data breach *(R.C. 1354.02)*.	Requires a covered entity seeking an affirmative defense under the bill to create, maintain, and comply with a written cybersecurity program that meets the bill's requirements, including requirements regarding the features, scale, and scope of the program and a requirement that the program *reasonably* comply with an industry *recognized* cybersecurity framework listed in the bill. States that a covered entity that complies with those requirements is entitled to assert an affirmative defense to any cause of action sounding in tort that is brought under the laws of Ohio or in the courts of Ohio and that alleges that the failure to implement reasonable information security controls resulted in a data breach *(R.C. 1354.02)*.
Industry recognized cybersecurity frameworks	Defines "NIST Cybersecurity Framework" as the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology, as updated from time to time, and requires a covered entity seeking an affirmative defense to comply with that framework or another framework listed in the bill *(R.C. 1354.01(E)).* Specifies that a covered entity must be deemed to be in compliance with the section of law that	Specifies that a covered entity's cybersecurity program, as described in the section of law that creates the affirmative defense, reasonably complies with an industry recognized cybersecurity framework for purposes of that section if either of the following apply: - The cybersecurity program reasonably complies with the current version of any of the following or any combination of the following: o The Framework for Improving

Topic	Previous Version (As Introduced)	Sub. Version (L_132_0943-5)
	creates the affirmative defense if any of the following apply: - The covered entity's cybersecurity program complies with the NIST Cybersecurity Framework. - The covered entity is in substantial compliance with any of the following: ○ NIST Special Publication 800-171; ○ NIST Special Publications 800-53 and 800-53a; ○ The Federal Risk and Authorization Management Program; ○ Center for Internet Security Critical Security Controls; ○ International Organization for Standardization/International Electrotechnical Commission 27000 Family – Information Security Management Systems. - The covered entity is regulated by the state and the federal government and is in substantial compliance with the entirety of any of the following: ○ The security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA); ○ Title V of the Gramm-Leach-Bliley Act of 1999; ○ The Federal Information Security	Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology (NIST); ○ NIST Special Publication 800-171; ○ NIST Special Publications 800-53 and 800-53a; ○ The Federal Risk and Authorization Management Program (FedRAMP) Security Assessment Framework; ○ The Center for Internet Security Critical Security Controls for Effective Cyber Defense; ○ The International Organization for Standardization/International Electrotechnical Commission 27000 Family – Information Security Management Systems. - The covered entity is regulated by the state, by the federal government, or both, and the cybersecurity program reasonably complies with the entirety of the current version of any of the following: ○ The security requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA); ○ Title V of the Gramm-Leach-Bliley Act of 1999; ○ The Federal Information Security

Topic	Previous Version (As Introduced)	Sub. Version (L_132_0943-5)
	Modernization Act of 2014. Specifies that, following any update to the NIST Cybersecurity Framework, or other industry recognized data security framework, covered entity has a period of one year from the stated effective date as prescribed in the framework to comply with the update *(R.C. 1354.02(D) and 1354.03)*.	Modernization Act of 2014. Specifies that when a final revision to a framework in the first list above is published, a covered entity whose cybersecurity program reasonably complies with that framework must reasonably comply with the revised framework not later than one year after the publication date stated in the revision. Specifies that when a framework in the second list above is amended, a covered entity whose cybersecurity program reasonably complies with that framework must reasonably comply with the amended framework not later than one year after the effective date of the amended framework *(R.C. 1354.03)*.
Intent statement	States that the purpose of the bill is to establish a legal safe harbor to be pled as an affirmative defense to a cause of action sounding in tort that alleges the failure to implement reasonable information security controls resulted in a data breach. Provides that the safe harbor applies to all covered entities that implement a cybersecurity program that complies with the Framework for Improving Critical Infrastructure Cybersecurity developed by the National Institute of Standards and Technology, or other industry recognized data security framework. Specifies that the bill must not be read to impose liability upon businesses that do not obtain or	States that the purpose of the bill is to establish a legal safe harbor to be pled as an affirmative defense to a cause of action sounding in tort that alleges *or relates to* the failure to implement reasonable information security controls, *resulting* in a data breach. Provides that the safe harbor applies to all covered entities that implement a cybersecurity program that meets the requirements of the bill. Specifies that the bill must not be read to impose liability upon businesses that do not obtain or maintain practices in compliance with the bill *(Section 2 of the bill)*.

Topic	Previous Version (As Introduced)	Sub. Version (L_132_0943-5)
	maintain practices in compliance with those frameworks *(Section 2 of the bill)*.	
Technical changes	Defines "individual" as a natural person. Defines "person" as an individual, corporation, business trust, estate, trust, partnership, association, or other legal entity that conducts business in Ohio *(R.C. 1354.01(D) and (F))*.	Eliminates the definition of "individual" and substitutes "natural person" for "individual" in the only provision of the bill that uses that term. Removes the definition of "person" because that term is not used in the bill *(R.C. 1354.01(D) and (F) and 1354.02(B)(3))*.

S0220-5-132/ec