4.4.4 Amend the Sarbanes-Oxley Act to Include Cybersecurity Reporting Requirements and Require Regular Pen Testing

Introduction to Proposal. This proposal harmonizes and clarifies cybersecurity oversight and reporting requirements for publicly traded companies by amending the Sarbanes-Oxley Act to explicitly account for cybersecurity oversight and resiliency measures, and require Pen Testing. It is designed to ensure that the resilience of publicly traded critical infrastructure owners and operators is elevated to the chief executive and/or board level.

Legend. This proposal would amend existing laws, and therefore changes are highlighted.

A BILL

To harmonize and clarify cybersecurity oversight and reporting requirements for publicly traded companies, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SEC. 1. DEFINITIONS.

Section 2 of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7201), is amended by inserting at the end the following:

"(18) CRITICAL INFORMATION SYSTEM.—The term "critical information system" means a set of activities, involving people, processes, data, or technology, which enable the issuer to obtain, generate, use, and communicate transactions and information in pursuit of core business objectives.

"(19) INFORMATION SECURITY CONTROL.—The term "information security control" means a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

"(20) CYBERSECURITY RISK.—The term "cybersecurity risk" means a significant vulnerability to, or a significant deficiency in, the security and defense activities of an information system."

SEC. 2. CORPORATE RESPONSIBILITY FOR FINANCIAL REPORTS AND CRITICAL INFORMATION SYSTEMS.

(a) IN GENERAL.—Section 302 of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7241) is amended—

(1) in the section heading, by inserting “and critical information systems” after “reports”;

(2) in subsection (a)—

(A) by inserting “, and the principal security, risk, or information security officer or officers” after “the principal financial officer or officers”;

(B) in paragraph (4)(A), by inserting “, including information security controls” after “internal controls”;

(C) in paragraph (4)(B), by inserting “, including information security controls,” after “internal controls”;

(D) in paragraph (4)(C), by inserting “, including information security controls,” after “internal controls”;

(E) in paragraph (4)(D), by inserting “, including information security controls,” after “internal controls”;

(F) in paragraph (5)(A), by inserting “and any significant cybersecurity risks in issuer's critical information systems” after “internal controls”; and

(G) in paragraph (6)—

(i) by inserting “, including information security controls,” after “significant changes in internal controls”;

(ii) by inserting “, including information security controls,” after “could significantly affect internal controls”; and

(iii) by inserting “cybersecurity risks,” before “significant deficiencies”.

(b) Clerical Amendment.—The table of contents of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7201) is amended by striking the item relating to section 302 and inserting the following new item:

“302. Corporate responsibility for financial reports and critical information systems.”.

SEC. 3. MANAGEMENT ASSESSMENTS OF INTERNAL CONTROLS AND CRITICAL INFORMATION SYSTEMS.

(a) In General.—Section 404 of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7241) is amended—

(1) in the section heading, by inserting "and critical information systems" after "controls";

(2) in subsection (a)—

(A) by redesignating paragraph (2) as paragraph (3);

(B) by inserting after paragraph (1) the following new paragraph (2);

"(2) state the responsibility of management for establishing and maintaining adequate internal information security controls, to include penetration testing, as applicable."; and

(C) in paragraph (3), as so redesignated by striking "of the issuer for financial reporting" and inserting "for financial reporting and the internal information security controls of the issuer";

(3) by redesignating subsection (c) as subsection (d);

(4) by inserting after subsection (b) the following new subsection (c):

"(c) **Information security control evaluation and reporting.** With respect to the internal information security control assessment required by subsection (a), any third-party information security firm that prepares or issues a cyber or information security risk assessment for the issuer, other than an issuer that is an emerging growth company (as defined in section 78c of this title), shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.";

(5) in subsection (d), by inserting "and (c)" after "Subsection (b)"; and

(6) by inserting after subsection (d) the following new subsection (e):

"(e) **Guidance on information security reporting**. The Commission shall issue guidance on how to describe information security issues in a way that does not compromise the reporting entity's security controls.".

(b) CLERICAL AMENDMENT.—The table of contents of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7241) is amended by striking the item relating to section 404 and inserting the following new item:

"404. Management assessment of internal controls and critical information systems.".

---

§ 2. Definitions

Except as otherwise specifically provided in this Act, in this Act, the following definitions shall apply:

(1) Appropriate State regulatory authority. The term "appropriate State regulatory authority" means the State agency or other authority responsible for the licensure or other regulation of the practice of accounting in the State or States having jurisdiction over a registered public accounting firm or associated person thereof, with respect to the matter in question.

(2) Audit. The term "audit" means an examination of the financial statements of any issuer by an independent public accounting firm in accordance with the rules of the Board or the Commission (or, for the period preceding the adoption of applicable rules of the Board under section 103 [*15 USCS § 7213*], in accordance with then-applicable generally accepted auditing and related standards for such purposes), for the purpose of expressing an opinion on such statements.

(3) Audit committee. The term "audit committee" means—

(A) a committee (or equivalent body) established by and amongst the board of directors of an issuer for the purpose of overseeing the accounting, and financial reporting processes of the issuer and audits of the financial statements of the issuer; and

(B) if no such committee exists with respect to an issuer, the entire board of directors of the issuer.

(4) Audit report. The term "audit report" means a document or other record—

(A) prepared following an audit performed for purposes of compliance by an issuer with the requirements of the securities laws; and

(B) in which a public accounting firm either—

(i) sets forth the opinion of that firm regarding a financial statement, report, or other document; or

(ii) asserts that no such opinion can be expressed.

(5) Board. The term "Board" means the Public Company Accounting Oversight Board established under section 101 [*15 USCS § 7211*].

(6) Commission. The term "Commission" means the Securities and Exchange Commission.

(7) Issuer. The term "issuer" means an issuer (as defined in section 3 of the Securities Exchange Act of 1934 (*15 U.S.C. 78c*)), the securities of which are registered under section 12 of that Act (*15 U.S.C. 78l*), or that is required to file reports under section 15(d) (*15 U.S.C. 78o(d)*), or that files or has filed a registration statement that has not yet become effective under the Securities Act of 1933 (*15 U.S.C. 77a* et seq.), and that it has not withdrawn.

(8) Non-audit services. The term "non-audit services" means any professional services provided to an issuer by a registered public accounting firm, other than those provided to an issuer in connection with an audit or a review of the financial statements of an issuer.

(9) Person associated with a public accounting firm.

(A) In general. The terms "person associated with a public accounting firm" (or with a "registered public accounting firm") and "associated person of a public accounting firm" (or of a "registered public accounting firm") mean any individual proprietor, partner, shareholder, principal, accountant, or other professional employee of a public accounting firm, or any other independent contractor or entity that, in connection with the preparation or issuance of any audit report—

(i) shares in the profits of, or receives compensation in any other form from, that firm; or

(ii) participates as agent or otherwise on behalf of such accounting firm in any activity of that firm.

(B) Exemption authority. The Board may, by rule, exempt persons engaged only in ministerial tasks from the definition in subparagraph (A), to the extent that the Board determines that any such exemption is consistent with the purposes of this Act, the public interest, or the protection of investors.

(C) Investigative and enforcement authority. For purposes of sections 3(c), 101(c), 105, and 107(c) [*15 USCS § 7202(c)*, *7211(c)*, *7215*, and *7217(c)*] and the rules of the Board and Commission issued thereunder, except to the extent specifically excepted by such rules, the terms defined in subparagraph (A) shall include any person associated, seeking to become associated, or formerly associated with a public accounting firm, except that—

(i) the authority to conduct an investigation of such person under section 105(b) [*15 USCS § 7215(b)*] shall apply only with respect to any act or practice, or omission to act, by the person while such person was associated or seeking to become associated with a registered public accounting firm; and

(ii) the authority to commence a disciplinary proceeding under section 105(c)(1) [*15 USCS § 7215(c)(1)*], or impose sanctions under section 105(c)(4) [*15 USCS § 7215(c)(4)*], against such person shall apply only with respect to—

(I) conduct occurring while such person was associated or seeking to become associated with a registered public accounting firm; or

(II) non-cooperation, as described in section 105(b)(3) [*15 USCS § 7215(b)(3)*], with respect to a demand in a Board investigation for testimony, documents, or other information relating to a period when such person was associated or seeking to become associated with a registered public accounting firm.

(10) Professional standards. The term "professional standards" means—

(A) accounting principles that are—

(i) established by the standard setting body described in section 19(b) of the Securities Act of 1933 [*15 USCS § 77s(b)*], as amended by this Act, or prescribed by the Commission under section 19(a) of that Act (15 U.S.C. 17a(s) [77s(a)] [*15 USCS § 77s(a)*]) or section 13(b) of the Securities Exchange Act of 1934 (*15 U.S.C. 78a(m)* [78m(b)] [*15 USCS § 78m(b)*]); and

(ii) relevant to audit reports for particular issuers, or dealt with in the quality control system of a particular registered public accounting firm; and

(B) auditing standards, standards for attestation engagements, quality control policies and procedures, ethical and competency standards, and independence standards (including rules implementing title II) that the Board or the Commission determines—

(i) relate to the preparation or issuance of audit reports for issuers; and

(ii) are established or adopted by the Board under section 103(a) [*15 USCS § 7213(a)*], or are promulgated as rules of the Commission.

(11) Public accounting firm. The term "public accounting firm" means—

(A) a proprietorship, partnership, incorporated association, corporation, limited liability company, limited liability partnership, or other legal entity that is engaged in the practice of public accounting or preparing or issuing audit reports; and

(B) to the extent so designated by the rules of the Board, any associated person of any entity described in subparagraph (A).

(12) Registered public accounting firm. The term "registered public accounting firm" means a public accounting firm registered with the Board in accordance with this Act.

(13) Rules of the Board. The term "rules of the Board" means the bylaws and rules of the Board (as submitted to, and approved, modified, or amended by the Commission, in accordance with section 107 [*15 USCS §*

7217]), and those stated policies, practices, and interpretations of the Board that the Commission, by rule, may deem to be rules of the Board, as necessary or appropriate in the public interest or for the protection of investors.

(14) Security. The term "security" has the same meaning as in section 3(a) of the Securities Exchange Act of 1934 (*15 U.S.C. 78c(a)*).

(15) Securities laws. The term "securities laws" means the provisions of law referred to in section 3(a)(47) of the Securities Exchange Act of 1934 (*15 U.S.C. 78c(a)(47)*), as amended by this Act, and includes the rules, regulations, and orders issued by the Commission thereunder.

(16) State. The term "State" means any State of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, or any other territory or possession of the United States.

(17) Foreign auditor oversight authority. The term "foreign auditor oversight authority" means any governmental body or other entity empowered by a foreign government to conduct inspections of public accounting firms or otherwise to administer or enforce laws related to the regulation of public accounting firms.

(18) Critical Information System.—The term "critical information system" means a set of activities, involving people, processes, data, or technology, which enable the issuer to obtain, generate, use, and communicate transactions and information in pursuit of core business objectives.

(19) Information Security Control.—The term "information security control" means a safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

(20) Cybersecurity Risk.—The term "cybersecurity risk" means a significant vulnerability to, or a significant deficiency in, the security and defense activities of an information system.".

§ 302. Corporate responsibility for financial reports and critical information systems

(a) Regulations required. The Commission shall, by rule, require, for each company filing periodic reports under section 13(a) or 15(d) of the Securities Exchange Act of 1934 (*15 U.S.C. 78m*, *78o(d)*), that the principal executive officer or officers and the principal financial officer or officers, and the principal security, risk, or information security officer or officers or persons performing similar functions, certify in each annual or quarterly report filed or submitted under either such section of such Act that—

(1) the signing officer has reviewed the report;

(2) based on the officer's knowledge, the report does not contain any untrue statement of a material fact or omit to state a material fact necessary in order to make the statements made, in light of the circumstances under which such statements were made, not misleading;

(3) based on such officer's knowledge, the financial statements, and other financial information included in the report, fairly present in all material respects the financial condition and results of operations of the issuer as of, and for, the periods presented in the report;

(4) the signing officers—

(A) are responsible for establishing and maintaining internal controls, including information security controls;

(B) have designed such internal controls, including information security controls, to ensure that material information relating to the issuer and its consolidated subsidiaries is made known to such officers by others within those entities, particularly during the period in which the periodic reports are being prepared;

(C) have evaluated the effectiveness of the issuer's internal controls, including including information security controls, as of a date within 90 days prior to the report; and

(D) have presented in the report their conclusions about the effectiveness of their internal controls, including information security controls, based on their evaluation as of that date;

(5) the signing officers have disclosed to the issuer's auditors and the audit committee of the board of directors (or persons fulfilling the equivalent function)—

(A) all significant deficiencies in the design or operation of internal controls which could adversely affect the issuer's ability to record, process, summarize, and report financial data and have identified for the issuer's auditors any material weaknesses in internal controls and any significant cybersecurity risks in issuer's critical information systems; and

(B) any fraud, whether or not material, that involves management or other employees who have a significant role in the issuer's internal controls; and

(6) the signing officers have indicated in the report whether or not there were significant changes in internal controls, including information security controls, or in other factors that could significantly affect internal controls, including information security controls, subsequent to the date of their evaluation, including any corrective actions with regard to cybersecurity risks, significant deficiencies and material weaknesses.

(b) Foreign reincorporations have no effect. Nothing in this section 302 [this section] shall be interpreted or applied in any way to allow any issuer to lessen the legal force of the statement required under this section 302 [this section], by an issuer having reincorporated or having engaged in any other transaction that resulted in the transfer of the corporate domicile or offices of the issuer from inside the United States to outside of the United States.

(c) Deadline. The rules required by subsection (a) shall be effective not later than 30 days after the date of enactment of this Act [enacted July 30, 2002].

§ 404. Management assessment of internal controls and critical information systems

(a) Rules required. The Commission shall prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 (*15 U.S.C. 78m* or *78o(d)*) to contain an internal control report, which shall—

(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and

(2) state the responsibility of management for establishing and maintaining adequate internal information security controls, to include penetration testing, as applicable.

(3) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures ~~of the issuer for financial reporting~~ for financial reporting and the internal information security controls of the issuer.

(b) Internal control evaluation and reporting. With respect to the internal control assessment required by subsection (a), each registered public accounting firm that prepares or issues the audit report for the issuer, other than an issuer that is an emerging growth company (as defined in section 3 of the Securities Exchange Act of 1934 [*15 USCS § 78c*]), shall attest to, and report on, the assessment made by the management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

(c) Information security control evaluation and reporting. With respect to the internal information security control assessment required by subsection (a), any third-party information security firm that prepares or issues a cyber or information security risk assessment for the issuer, other than an issuer that is an emerging growth company (as defined in section 78c of this title), shall attest to, and report on, the assessment made by the

management of the issuer. An attestation made under this subsection shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

(d) Exemption for smaller issuers. Subsection (b) and (c) shall not apply with respect to any audit report prepared for an issuer that is neither a "large accelerated filer" nor an "accelerated filer" as those terms are defined in Rule 12b-2 of the Commission (*17 C.F.R. 240.12b-2*).

(e) Guidance on information security reporting. The Commission shall issue guidance on how to describe information security issues in a way that does not compromise the reporting entity's security controls.