I

114TH CONGRESS
2D SESSION

H. R. 5069

To amend the Sarbanes-Oxley Act of 2002 to protect investors by expanding the mandated internal controls reports and disclosures to include cybersecurity systems and risks of publicly traded companies.

IN THE HOUSE OF REPRESENTATIVES

APRIL 26, 2016

Mr. MCDERMOTT introduced the following bill; which was referred to the Committee on Financial Services

---

A BILL

To amend the Sarbanes-Oxley Act of 2002 to protect investors by expanding the mandated internal controls reports and disclosures to include cybersecurity systems and risks of publicly traded companies.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Cybersecurity Systems and Risks Reporting Act''.

SEC. 2. CYBERSECURITY AND INFORMATION SYSTEM REQUIREMENTS.

(a) DEFINITIONS.—Section 2(a) of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7201(a)) is amended—

(1) in paragraph (2), by inserting after ''financial statements'' the following: ''and information systems'';

(2) in paragraph (3)(A), by striking ''and financial'' and inserting '', financial, and cybersecurity systems'';

(3) in paragraph (10)(B), by inserting after ''quality control policies and procedures,'' the following: ''cybersecurity systems standards and practices,''; and

(4) by adding at the end the following:

''(18) INFORMATION SYSTEM.—The term '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 to maintain accountability and measure and review the issuer's performance or progress towards achievement of objectives.

''(19) CYBERSECURITY SYSTEM.—The term 'cybersecurity system' means a set of activities or state, involving people, processes, data or technology, whereby the protection of an information system of

the issuer is secured from, or defended against, damage, unauthorized use or modification, misdirection, disruption or exploitation.

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

(b) CORPORATE RESPONSIBILITY.—Section 302 of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7241) is amended—

(1) in the heading of such section, by inserting after ''**REPORTS**'' the following: ''**AND INFORMATION SYSTEMS**''; and

(2) in subsection (a)—

(A) by striking ''and the principal financial officer or officers,'' and inserting '', the principal financial officer or officers, and the principal cybersecurity systems officer or officers'';

(B) in paragraph (4), by striking ''internal controls'' each place such term appears and inserting ''internal controls and cybersecurity systems'';

(C) in paragraph (5)—

(i) in subparagraph (A)—

(I) by inserting after ''operation of internal controls'' the following: ''and cybersecurity systems''; and

(II) by inserting before the semicolon the following: ''and any significant cybersecurity risks in issuer's information systems''; and

(ii) in subparagraph (B), by inserting before the semicolon the following: '', cybersecurity systems, or information systems''; and

(D) in paragraph (6)—

(i) by striking ''internal controls'' each place such term appears and inserting ''internal controls, cybersecurity systems, or information systems''; and

(ii) by striking ''significant deficiencies'' and inserting ''cybersecurity risks, significant deficiencies,''.

(c) MANAGEMENT ASSESSMENT.—Section 404 of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7262) is amended—

(1) in the heading of such section, by inserting after ''**CONTROLS**'' the following: ''**AND INFORMATION SYSTEMS**'';

(2) in subsection (a)—

(A) by inserting after ''contain an internal control'' the following: ''and information systems'';

(B) in paragraph (1), by striking ''an adequate internal control structure and procedures for financial reporting'' and inserting ''adequate internal control and cybersecurity systems structures and procedures for financial and information systems reporting''; and

(C) by amending paragraph (2) to read as follows:

''(2) contain assessments, as of the end of the most recent fiscal year of the issuer, of the effectiveness of—

''(A) the internal control structure and procedures of the issuer for financial reporting; and

''(B) the cybersecurity systems structure of the issuer.''; and

(3) in subsection (b)—

(A) in the heading of such subsection, by inserting after ''INTERNAL CONTROL'' the following; ''AND CYBERSECURITY SYSTEMS''; and

(B) by striking ''internal control assessment'' and inserting ''internal control and cybersecurity system structure assessments''.

(d) DISCLOSURE OF EXPERT.—Section 407 of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7265) is amended—

(1) in the heading of such section, by striking ''**EXPERT**'' and inserting ''**AND CYBERSECURITY SYSTEMS EXPERTS**'';

(2) in subsection (a)—

(A) in the heading of such subsection, by striking ''EXPERT'' and inserting ''AND CYBERSECURITY EXPERTS''; and

(B) by striking '', as such term is defined by the Commission'' and inserting ''and at least 1 member who is a cybersecurity systems expert, as such terms are defined by the Commission in consultation with the Secretary of Homeland Security and the Secretary of Commerce''; and

(3) by striking subsection (c) and inserting the following:

''(c) CONSIDERATIONS WITH RESPECT TO CYBERSECURITY EXPERTS.—In defining the term 'cybersecurity expert' for purposes of subsection (a), the Commission

shall, in consultation with the Secretary of Homeland Security and the Secretary of Commerce, consider whether a person has, through education or experience as an information technology officer or information systems security officer, or from a position involving the performance of similar functions—

''(1) an understanding of generally accepted principles, practices, and law relating to computer security, computer network security, and data security and privacy;

''(2) experience in—

''(A) the preparation of information systems audits for cybersecurity risk discovery; and

''(B) the maintenance, implementation, and monitoring of information systems and their cybersecurity systems;

''(3) experience with information systems aspects of internal accounting controls; and

''(4) an understanding of audit committee functions.''.

(e) ENHANCED REVIEW.—Section 408 of the Sarbanes-Oxley Act of 2002 (15 U.S.C. 7265) is amended—

(1) in subsection (a), by striking ''financial statement'' and inserting ''financial, information systems, and cybersecurity systems statements''; and

(2) in subsection (b)—

(A) in paragraph (5), by striking ''and'' at the end;

(B) by redesignating paragraph (6) as paragraph (7); and

(C) by inserting after paragraph (5) the following:

''(6) issuers that have issued cybersecurity risks disclosures; and''.

(f) CLERICAL AMENDMENT.—The table of contents in section 1(b) of the Sarbanes-Oxley Act of 2002 is amended—

(1) in the item relating to section 302, by inserting after ''REPORTS'' the following: ''AND INFORMATION SYSTEMS'';

(2) in the item relating to section 404, by inserting after ''CONTROLS'' the following: ''AND INFORMATION SYSTEMS''; and

(3) in the item relating to section 407, by striking ''EXPERT'' and inserting ''AND CYBERSECURITY SYSTEMS EXPERTS''.

○