AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

115TH CONGRESS
1ST SESSION

S. 536

To promote transparency in the oversight of cybersecurity risks at publicly traded companies.

IN THE SENATE OF THE UNITED STATES

MARCH 7, 2017

Mr. REED (for himself, Ms. COLLINS, and Mr. WARNER) introduced the following bill; which was read twice and referred to the Committee on Banking, Housing, and Urban Affairs

---

A BILL

To promote transparency in the oversight of cybersecurity risks at 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 Disclosure Act of 2017''.

SEC. 2. CYBERSECURITY TRANSPARENCY.

(a) DEFINITIONS.—In this section—

(1) the term ''Commission'' means the Securities and Exchange Commission;

(2) the term ''cybersecurity threat''—

(A) means an action, not protected by the First Amendment to the Constitution of the United States, on or through an information system that may result in an unauthorized effort to adversely impact the security, availability, confidentiality, or integrity of an information system or information that is stored on, processed by, or transiting an information system; and

(B) does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement;

(3) the term ''information system''—

(A) has the meaning given the term in section 3502 of title 44, United States Code; and

(B) includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers;

(4) the term ''issuer'' has the meaning given the term in section 3 of the Securities Exchange Act of 1934 (15 U.S.C. 78c);

(5) the term ''NIST'' means the National Institute of Standards and Technology; and

(6) the term ''reporting company'' means any company that is an issuer—

(A) the securities of which are registered under section 12 of the Securities Exchange Act of 1934 (15 U.S.C. 78l); or

(B) that is required to file reports under section 15(d) of such Act (15 U.S.C. 78o(d)).

(b) REQUIREMENT TO ISSUE RULES.—Not later than 360 days after the date of enactment of this Act, the Commission shall issue final rules to require each reporting company, in the annual report submitted under section 13 or section 15(d) of the Securities Exchange Act of 1934 (15 U.S.C. 78m and 78o(d)) or the annual proxy statement submitted under section 14(a) of such Act (15 U.S.C. 78n(a))—

(1) to disclose whether any member of the governing body, such as the board of directors or general partner, of the reporting company has expertise or experience in cybersecurity and in such detail as necessary to fully describe the nature of the expertise or experience; and

(2) if no member of the governing body of the reporting company has expertise or experience in cybersecurity, to describe what other cybersecurity steps taken by the reporting company were taken

into account by such persons responsible for identifying and evaluating nominees for any member of the governing body, such as a nominating committee.

(c) CYBERSECURITY EXPERTISE OR EXPERIENCE.—For purposes of subsection (b), the Commission, in consultation with NIST, shall define what constitutes expertise or experience in cybersecurity, such as professional qualifications to administer information security program functions or experience detecting, preventing, mitigating, or addressing cybersecurity threats, using commonly defined roles, specialities, knowledge, skills, and abilities, such as those provided in NIST Special Publication 800–181 entitled ''NICE Cybersecurity Workforce Framework'', or any successor thereto.

○