

116TH CONGRESS
1ST SESSION

S. 592

To amend the Securities Exchange Act of 1934 to promote transparency in the oversight of cybersecurity risks at publicly traded companies.

IN THE SENATE OF THE UNITED STATES

FEBRUARY 28, 2019

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

A BILL

To amend the Securities Exchange Act of 1934 to promote transparency in the oversight of cybersecurity risks at publicly traded companies.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Cybersecurity Dislo-
5 sure Act of 2019”.

6 **SEC. 2. CYBERSECURITY TRANSPARENCY.**

7 The Securities Exchange Act of 1934 (15 U.S.C. 78a
8 et seq.) is amended by inserting after section 14B (15
9 U.S.C. 78n–2) the following:

1 **“SEC. 14C. CYBERSECURITY TRANSPARENCY.**

2 “(a) DEFINITIONS.—In this section—

3 “(1) the term ‘cybersecurity’ means any action,
4 step, or measure to detect, prevent, deter, mitigate,
5 or address any cybersecurity threat or any potential
6 cybersecurity threat;

7 “(2) the term ‘cybersecurity threat’—

8 “(A) means an action, not protected by the
9 First Amendment to the Constitution of the
10 United States, on or through an information
11 system that may result in an unauthorized ef-
12 fort to adversely impact the security, avail-
13 ability, confidentiality, or integrity of an infor-
14 mation system or information that is stored on,
15 processed by, or transiting an information sys-
16 tem; and

17 “(B) does not include any action that sole-
18 ly involves a violation of a consumer term of
19 service or a consumer licensing agreement;

20 “(3) the term ‘information system’—

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

24 “(B) includes industrial control systems,
25 such as supervisory control and data acquisition

1 systems, distributed control systems, and pro-
2 grammable logic controllers;

3 “(4) the term ‘NIST’ means the National Insti-
4 tute of Standards and Technology; and

5 “(5) the term ‘reporting company’ means any
6 company that is an issuer—

7 “(A) the securities of which are registered
8 under section 12; or

9 “(B) that is required to file reports under
10 section 15(d).

11 “(b) REQUIREMENT TO ISSUE RULES.—Not later
12 than 360 days after the date of enactment of this section,
13 the Commission shall issue final rules to require each re-
14 porting company, in the annual report of the reporting
15 company submitted under section 13 or section 15(d) or
16 in the annual proxy statement of the reporting company
17 submitted under section 14(a)—

18 “(1) to disclose whether any member of the
19 governing body, such as the board of directors or
20 general partner, of the reporting company has exper-
21 tise or experience in cybersecurity and in such detail
22 as necessary to fully describe the nature of the ex-
23 pertise or experience; and

24 “(2) if no member of the governing body of the
25 reporting company has expertise or experience in cy-

1 bersecurity, to describe what other aspects of the re-
2 porting company’s cybersecurity were taken into ac-
3 count by any person, such as an official serving on
4 a nominating committee, that is responsible for iden-
5 tifying and evaluating nominees for membership to
6 the governing body.

7 “(c) CYBERSECURITY EXPERTISE OR EXPERI-
8 ENCE.—For purposes of subsection (b), the Commission,
9 in consultation with NIST, shall define what constitutes
10 expertise or experience in cybersecurity using commonly
11 defined roles, specialties, knowledge, skills, and abilities,
12 such as those provided in NIST Special Publication 800–
13 181, entitled ‘National Initiative for Cybersecurity Edu-
14 cation (NICE) Cybersecurity Workforce Framework’, or
15 any successor thereto.”.

○