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

IN THE HOUSE OF REPRESENTATIVES
MARCH 13, 2019
Mr. Himes (for himself, Mr. Heck, and Mr. Meeks) introduced the following bill; which was referred to the Committee on Financial Services

A BILL
To amend the Securities Exchange Act of 1934 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 2019”.

SEC. 2. CYBERSECURITY TRANSPARENCY.
“SEC. 14C. CYBERSECURITY TRANSPARENCY.

“(a) DEFINITIONS.—In this section—

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

“(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 pro-
grammable logic controllers;

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

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

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

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

“(b) Requirement To Issue Rules.—Not later
than 360 days after the date of enactment of this section,
the Commission shall issue final rules to require each re-
porting company, in the annual report of the reporting
company submitted under section 13 or section 15(d) or
in the annual proxy statement of the reporting company
submitted under section 14(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 exper-
tise or experience in cybersecurity and in such detail
as necessary to fully describe the nature of the ex-
pertise or experience; and

“(2) if no member of the governing body of the
reporting company has expertise or experience in cy-
bersecurity, to describe what other aspects of the reporting company’s cybersecurity were taken into account by any person, such as an official serving on a nominating committee, that is responsible for identifying and evaluating nominees for membership to the governing body.

“(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 using commonly defined roles, specialties, knowledge, skills, and abilities, such as those provided in NIST Special Publication 800–181, entitled ‘National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework’, or any successor thereto.”