AMENDMENT TO RULES COMMITTEE PRINT 116-57

OFFERED BY MR. HIMES OF CONNECTICUT

Page 1115, after line 5, insert the following:

SEC. 17. CYBERSECURITY TRANSPARENCY.


"SEC. 14C. CYBERSECURITY TRANSPARENCY."

"(a) Rulemaking.—

"(1) In general.—The Commission shall, not later than 360 days after the date of enactment of this section, issue a final rule requiring each reporting company—

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

"(B) if no member of the governing body of the reporting company has expertise or expe-
rience in cybersecurity, to describe what other aspects of the reporting company’s cybersecurity were considered 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.

“(2) DISCLOSURES.—The disclosures required under paragraph (1) shall be made 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).

“(b) CYBERSECURITY EXPERTISE OR EXPERIENCE.—For purposes of subsection (a), the Commission, in consultation with NIST, shall define what constitutes expertise or experience in cybersecurity based on 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.

“(c) DEFINITIONS.—For purposes of this section:

“(1) CYBERSECURITY.—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) CYBERSECURITY THREAT.—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) INFORMATION SYSTEM.—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) NIST.—The term ‘NIST’ means the National Institute of Standards and Technology.

“(5) REPORTING COMPANY.—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).”.

□