116TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
116–633

CYBERSECURITY DISCLOSURE ACT OF 2019

DECEMBER 8, 2020.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

Ms. WATERS, from the Committee on Financial Services, submitted the following

R E P O R T

together with

MINORITY VIEWS

[To accompany H.R. 1731]

[Including cost estimate of the Congressional Budget Office]

The Committee on Financial Services, to whom was referred the bill (H.R. 1731) to amend the Securities Exchange Act of 1934 to promote transparency in the oversight of cybersecurity risks at publicly traded companies, having considered the same, reports favorably thereon with an amendment and recommends that the bill as amended do pass.

CONTENTS

19–006

The amendment is as follows:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cybersecurity Disclosure Act of 2019".

SEC. 2. CYBERSECURITY TRANSPARENCY.

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

"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 programmable logic controllers;

"(4) the term 'NIST' means the National Institute 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 reporting 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 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 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, titled 'National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework', or any successor thereto.".

PURPOSE AND SUMMARY

On March 13, 2019, Representative Jim Himes introduced H.R. 1731, the Cybersecurity Disclosure Act of 2019. H.R. 1731, which would require the Securities and Exchange Commission (SEC) to issue rules that require publicly traded companies, in their annual reports to the SEC or in their annual proxy statements, to disclose whether any member of the company's board of directors, or similar governing body, has expertise or experience in cybersecurity and the nature of such expertise or experience. If no members of the company's governing body have cybersecurity experience or expertise, the bill would require the company to describe what other cy-

bersecurity aspects were taken into account by persons responsible for identifying and evaluating nominees for the company's governing body.

BACKGROUND AND NEED FOR LEGISLATION

According to Deloitte Touche Tohmatsu Limited's 2019 global risk management survey of financial institutions, "[s]ixty-seven percent of respondents named cybersecurity as one of the three risks that would increase the most in importance for their business over the next two years, far more than for any other risk." [1] However, "only about one-half of the respondents felt their institutions were extremely effective or very effective in managing this risk." Moreover, according to the Identity Theft Resource Center and CyberScout, breaches that exposed records containing consumers' personally identifiable information rose 126%, from 2017 to 2018.[2] H.R. 1731 faciliates transparency into publicly traded companies' cybersecurity risks and helps ensure that both consumers and investors will be informed of the human resources available to address such risks.

The bill is supported by consumer advocates, investors, and securities law experts, including the North American Securities Administrators Association; the Council of Institutional Investors; the National Association of State Treasurers; the California Public Employees' Retirement System; the Bipartisan Policy Center; Massachusetts Institute of Technology Professor Simon Johnson; Harvard Law Professor John Coates; Columbia Law Professor Jack Coffee; K&L Gates LLP; and the Consumer Federation of America.

This bill is similar to a bipartisan bill in the Senate, S. 592, which is sponsored by Senators Reed, Collins, and Kennedy.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

This section states that the title of the bill is the "Cyber Security Disclosure Act of 2019."

Section 2. Cybersecurity transparency

Section 2 amends the Securities Exchange Act of 1934 (15 U.S.C. 78a) by adding a new section 14C to the Act. The new section 14C requires issuers that have registered securities or that file annual reports to disclose in any proxy or consent solicitation material for an annual shareholder meeting: a clear description of the link between environmental, social, and governance (ESG) metrics and the issuer's long-term business strategy; and any process the issuer uses to determine the impact of these ESG metrics on its long-term business strategy.

Paragraph (1) of subsection (a) of the new section 14C defines the term 'cybersecurity' as any action, step, or measure to detect, prevent, deter, mitigate, or address any cybersecurity threat or any potential cybersecurity threat;

---

[1] Deloitte, Global risk management survey, 11th edition, Jan. 2019, https://www2.deloitte.com/us/en/insights/industry/financial-services/global-risk-management-survey-financial-services.html

[2] Identity Theft Resource Center, 2018 End-of-Year Data Breach Report, https://www.idtheftcenter.org/2018-end-of-year-data-breach-report/

Paragraph (2) of subsection (a) defines the term 'cybersecurity threat' as an action 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. The subsection clarifies that the term 'cybersecurity threat' does not include any action that solely involves a violation of a consumer term of service or a consumer licensing agreement. The subsection exempts actions that are protected by the First Amendment of the Constitution of the United States.

Paragraph (3) of subsection (a) assigns the same definition of 'information system' as that of 44 U.S.C. § 3502, which defines 'information system' as a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Paragraph (4) of subsection (a) defines the term 'NIST' as the National Institute of Standards and Technology.

Paragraph (5) of subsection (a) defines the term 'reporting company' as any company that is an issuer, the securities of which are registered under section 12; or that is required to file reports under 15(d).

Subsection (b) of the new section 14C requires the Securities and Exchange Commission to issue final rules that will require reporting companies, in their annual reports submitted under section 13 or section 15(d) or in their annual proxy statement submitted under 14(a), to disclose whether any member of the reporting company's governing body has expertise or experience in cybersecurity and to describe the nature of the expertise or experience. If no member of the governing body has expertise or experience in cybersecurity, the final rule will require the reporting company to describe what other aspects of the reporting company's cybersecurity were taken into account by individuals who are responsible for identifying and evaluating nominees for membership to the governing body.

Subsection (c) of the new Section 14C requires the Securities and Exchange Commission, in consultation with the NIST, to define what constitutes expertise or experience in cybersecurity using commonly defined roles, specialties, knowledge, skills, and abilities, such as those listed in NIST Special Publication 800–181, entitled "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," or any successor publication.

HEARINGS

For the purposes of section 103(i) of H. Res. 6 for the 116th Congress, the Committee on Financial Services' Subcommittee on Investor Protection, Entrepreneurship, and Capital Markets held a hearing on July 10, 2019 to consider H.R. 1731 entitled, "Building a Sustainable and Competitive Economy: An Examination of Proposals to Improve Environmental, Social and Governance Disclosures." Testifying at this hearing were Tim Mohin, Chief Executive at the Global Reporting Initiative; James Andrus, Investment Manager-Financial Markets, Sustainable Investment, CalPERS Investment Office; Paul Atkins, Chief Executive Officer, Patomak Global Partners; Degas Wright, CFA, Chief Executive Officer, Decatur

Capital Management, Inc.; and Mindy Lubber, President and Chief Executive Officer, Ceres.

COMMITTEE CONSIDERATION

The Committee on Financial Services met in open session on December 10, 2019, and ordered H.R. 1731 to be reported favorably to the House with an amendment in the nature of a substitute by a vote of 32 yeas and 24 nays, a quorum being present.

COMMITTEE VOTES AND ROLL CALL VOTES

In compliance with clause 3(b) of rule XIII of the Rules of the House of Representatives, the Committee advises that the following roll call votes occurred during the Committee's consideration of H.R. 1731.

Present	Representatives	Ayes	Nays
	Ms. Waters, *Chairwoman*	X	
	Mrs. Maloney	X	
	Ms. Velázquez	X	
	Mr. Sherman	X	
	Mr. Meeks	X	
	Mr. Clay	X	
	Mr. Scott		
	Mr. Green	X	
	Mr. Cleaver	X	
	Mr. Perlmutter	X	
	Mr. Himes	X	
	Mr. Foster	X	
	Mrs. Beatty	X	
	Mr. Heck	X	
	Mr. Vargas	X	
	Mr. Gottheimer	X	
	Mr. Gonzalez (TX)	X	
	Mr. Lawson	X	
	Mr. San Nicolas	X	
	Ms. Tlaib	X	
	Ms. Porter	X	
	Ms. Axne	X	
	Mr. Casten	X	
	Ms. Pressley	X	
	Mr. McAdams	X	
	Ms. Ocasio-Cortez	X	
	Ms. Wexton	X	
	Mr. Lynch	X	
	Ms. Gabbard		
	Ms. Adams	X	
	Ms. Dean	X	
	Mr. Garcia (IL)	X	
	Ms. Garcia (TX)	X	
	Mr. Phillips	X	
34			
	Mr. McHenry, *Ranking Member*		X
	Mrs. Wagner		X
	Mr. King		X
	Mr. Lucas		X
	Mr. Posey		X
	Mr. Luetkemeyer		X
	Mr. Huizenga		X
	Mr. Stivers		X
	Mr. Barr		X
	Mr. Tipton		X
	Mr. Williams		X
	Mr. Hill		X
	Mr. Emmer		X
	Mr. Zeldin		X
	Mr. Loudermilk		X
	Mr. Mooney		X
	Mr. Davidson		X
	Mr. Budd		X
	Mr. Kustoff		
	Mr. Hollingsworth		X
	Mr. Gonzalez (OH)		X
	Mr. Rose		X
	Mr. Steil		X
	Mr. Gooden		X
	Mr. Riggleman		X
	Mr. Timmons		X
26			

Committee on Financial Services

Full Committee

116th Congress (1st Session)

Date: 12/10/2019

Measure H.R. 1731

Amendment No.

Offered by: Mr. Himes, Final Passage

Agreed To	Yes	No	Prsnt	Wdrn

Voice Vote	Ayes	Nays

Record Vote	FC
	32 Ayes- 24 Noes

STATEMENT OF OVERSIGHT FINDINGS AND RECOMMENDATIONS OF THE COMMITTEE

In compliance with clause 3(c)(1) of rule XIII and clause 2(b)(1) of rule X of the Rules of the House of Representatives, the Committee's oversight findings and recommendations are reflected in the descriptive portions of this report.

STATEMENT OF PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause (3)(c) of rule XIII of the Rules of the House of Representatives, the goals of H.R. 1731 are to ensure that the Securities Exchange Act requires disclosures of whether companies have cybersecurity experience among key officers or board members.

NEW BUDGET AUTHORITY AND CBO COST ESTIMATE

Pursuant to clause 3(c)(2) of rule XIII of the Rules of the House of Representatives and section 308(a) of the *Congressional Budget Act of 1974*, and pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives and section 402 of the *Congressional Budget Act of 1974*, the Committee has received the following estimate for H.R. 1731 from the Director of the Congressional Budget Office:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC.

Hon. MAXINE WATERS,
Chairwoman, Committee on Financial Services,
House of Representatives, Washington, DC.

DEAR MADAM CHAIRWOMAN: The Congressional Budget Office has prepared the enclosed cost estimate for H.R. 1731, the Cybersecurity Disclosure Act of 2019.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is David Hughes.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

H.R. 1731, Cybersecurity Disclosure Act of 2019
As ordered reported by the House Committee on Financial Services on December 11, 2019

By Fiscal Year, Millions of Dollars	2020	2020-2025	2020-2030
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	*	*

Statutory pay-as-you-go procedures apply?	No	**Mandate Effects**	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2031?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	Yes, Under Threshold

* = between -$500,000 and $500,000.

H.R. 1731 would require the Securities and Exchange Commission (SEC) to issue rules that require publicly traded companies to report annually on whether members of their governing bodies (such as general partners or members of a board of directors) have cybersecurity expertise and the nature of that experience. If nobody has such experience, then the company would be required to describe what other aspects of its cybersecurity were considered by the people responsible for identifying and evaluating nominees for governing body membership. H.R. 1731 would require the SEC (in consultation with the National Institute of Standards and Technology) to define expertise or experience in cybersecurity.

For this estimate, CBO assumes that the bill will be enacted in fiscal year 2020. Based on the estimated costs of similar proposals, CBO estimates that it would cost the SEC less than $500,000 to issue rules over the 2020–2021 period. CBO expects that the work would require two employees, at an annual cost of $260,000 each, for less than a year. However, because the SEC is authorized to collect fees sufficient to offset its annual appropriation, CBO expects that the net effect on discretionary spending would be negligible, assuming appropriation actions consistent with that authority.

H.R. 1731 contains private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA). CBO estimates that the cost to comply with those mandates would be small and would not exceed the threshold established in UMRA ($168 million in 2020, adjusted annually for inflation).

By requiring publicly traded companies to annually disclose to the SEC the nature of their board members' experience in cyber security, H.R. 1731 would impose a mandate as defined in UMRA. The incremental cost of the mandate would be small because the mandated entities already collect or possess the information to be reported under the bill and would use an established reporting process.

If the SEC increased fees to offset the costs associated with implementing the bill, H.R. 1731 would increase the cost of an existing mandate on private entities required to pay those fees. CBO estimates that the incremental cost of the mandate would be small.

H.R. 1731 contains no intergovernmental mandates as defined in UMRA.

The CBO staff contact for this estimate is David Hughes (for federal costs) and Rachel Austin (for mandates). The estimate was reviewed by H. Samuel Papenfuss, Deputy Director of Budget Analysis.

COMMITTEE COST ESTIMATE

Clause 3(d)(1) of rule XIII of the Rules of the House of Representatives requires an estimate and a comparison of the costs that would be incurred in carrying out H.R. 1731. However, clause 3(d)(2)(B) of that rule provides that this requirement does not apply when the committee has included in its report a timely submitted cost estimate of the bill prepared by the Director of the Congressional Budget Office under section 402 of the *Congressional Budget Act*.

UNFUNDED MANDATE STATEMENT

Pursuant to Section 423 of the *Congressional Budget and Impoundment Control Act* (as amended by Section 101(a)(2) of the *Unfunded Mandates Reform Act*, Pub. L. 104–4), the Committee adopts as its own the estimate of federal mandates regarding H.R. 1731, as amended, prepared by the Director of the Congressional Budget Office.

ADVISORY COMMITTEE

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICATION OF LAW TO THE LEGISLATIVE BRANCH

Pursuant to section 102(b)(3) of the *Congressional Accountability Act*, Pub. L. No. 104–1, H.R. 1731, as amended, does not apply to terms and conditions of employment or to access to public services or accommodations within the legislative branch.

EARMARK STATEMENT

In accordance with clause 9 of rule XXI of the Rules of the House of Representatives, H.R. 1731 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as described in clauses 9(e), 9(f), and 9(g) of rule XXI.

DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII of the Rules of the House of Representatives, the Committee states that no provision of H.R. 1731 establishes or reauthorizes a program of the Federal Government known to be duplicative of another federal program, a program that was included in any report from the Government Accountability Office to Congress pursuant to section 21 of Public Law 111–139, or a program related to a program identified in the most recent Catalog of Federal Domestic Assistance.

CHANGES TO EXISTING LAW

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, H.R. 1731, as reported, are shown as follows:

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with clause 3(e) of rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (new matter is printed in italics and existing law in which no change is proposed is shown in roman):

SECURITIES EXCHANGE ACT OF 1934

TITLE I—REGULATION OF SECURITIES EXCHANGES

* * * * * * *

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 programmable logic controllers;

(4) the term "NIST" means the National Institute 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 reporting 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 report-

ing 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 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, titled "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework", or any successor thereto.

* * * * * * *

MINORITY VIEWS

American businesses face cybersecurity threats every day. Companies are prioritizing efforts to mitigate those threats. The Democrats only answer to strengthening corporate cybersecurity is another mandatory disclosure bill that will have no effect on a company's security efforts.

- H.R. 1731 will not help make companies more secure, help companies address cybersecurity risks, or even provide useful information to investors regarding a specific company's cybersecurity efforts. Instead, the bill may require companies to reveal vulnerabilities.
- The bill's mandated disclosure will ultimately raise a company's compliance costs, deterring companies from going public. Fewer public companies negatively impacts consumers' long-term investment opportunities such as saving for retirement or a child's education.

Committee Republicans understand that companies and their shareholders are best positioned to determine who should serve on boards of directors and the needs of their companies, particularly as those decisions relate to a company's cybersecurity efforts.

Some public companies should consider experienced cybersecurity experts for their boards, while other companies' cybersecurity concerns may be better handled at a different level of the business or even by a third-party service provider.

The SEC already requires significant disclosures relating to board nominations and elections.

- Item 401 of Regulation S–K[1] requires disclosure about the business experience of each director as well as the "experience, qualifications, or skill" that make the director appropriate for service. Cybersecurity concerns and risks that are relevant for a given board member is already required to be disclosed under current SEC requirements.
- In 2018, the SEC issued guidance that assists public companies in preparing disclosures about cybersecurity risks and incidents.[2] This guidance provides the SEC's views on a company's disclosure responsibilities on matters involving cybersecurity risk and incidents.

H.R. 1731 may require disclosure of "aspects of . . . cybersecurity" that were considered in board nominations. This language may be asking public companies to consider disclosing significant vulnerabilities—which would likely further open these companies up to cyber-attack.

The Democrats have held no hearings on the issue of cybersecurity. They have not consulted with regulators on this issue; nor

[1] 17 CFR § 229.401.

[2] *See* "Commission Statement and Guidance on Public Company Cybersecurity Disclosures" (Feb. 21, 2018), available at *https://www.sec.gov/rules/interp/2018/33-10459.pdf.*

have they held any bipartisan discussion about what resources are needed to strengthen a company's cybersecurity platform. The Democrats' solution to any corporate issue is to legislate mandatory disclosures.

Democrats' proposals will encourage more companies to go or stay private, depriving everyday Americans of investment opportunities and depriving companies of important sources of capital formation.

For these reasons, Committee Republicans are opposed to H.R. 1731.

ROGER WILLIAMS.
BARRY LOUDERMILK.
TREY HOLLINGSWORTH.
LANCE GOODEN.
DAVID KUSTOFF.
WILLIAM R. TIMMONS, IV.
SCOTT R. TIPTON.
WARREN DAVIDSON.
DENVER RIGGLEMAN.
ANDY BARR.
ANN WAGNER.
BLAINE LUETKEMEYER.
ALEXANDER X. MOONEY.
JOHN W. ROSE.
STEVE STIVERS.
J. FRENCH HILL.
VAN TAYLOR.
TOM EMMER.
TED BUDD.
BRYAN STEIL.
ANTHONY GONZALEZ.
FRANK D. LUCAS.
LEE M. ZELDIN.
BILL HUIZENGA.
BILL POSEY.
PATRICK T. MCHENRY.

○