118TH CONGRESS
2d Session
HOUSE OF REPRESENTATIVES
REPORT
118–727

PROVIDING FOR CONGRESSIONAL DISAPPROVAL UNDER CHAPTER 8 OF TITLE 5, UNITED STATES CODE, OF THE RULE SUBMITTED BY THE SECURITIES AND EXCHANGE COMMISSION RELATING TO "CYBERSECURITY RISK MANAGEMENT, STRATEGY, GOVERNANCE, AND INCIDENT DISCLOSURE"

NOVEMBER 1, 2024.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

Mr. MCHENRY, from the Committee on Financial Services, submitted the following

R E P O R T

together with

MINORITY VIEWS

[To accompany H.J. Res. 100]

[Including cost estimate of the Congressional Budget Office]

The Committee on Financial Services, to whom was referred the joint resolution (H.J. Res. 100) providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Securities and Exchange Commission relating to "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure", having considered the same, reports favorably thereon without amendment and recommends that the joint resolution do pass.

CONTENTS

59–006

PURPOSE AND SUMMARY

Introduced on November 11, 2023, by Representative Andrew Garbarino, H.J. Res. 100, a resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Securities and Exchange Commission relating to the "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure," would rescind the Securities and Exchange Commission's (SEC) rule "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."

BACKGROUND AND NEED FOR LEGISLATION

On July 26, 2023, the Securities and Exchange Commission ("SEC") voted 3–2 to adopt the Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rule ("the Cyber Rule" or "the Final Rule"). The Final Rule requires expansive new disclosures by public companies regarding cybersecurity matters, concerning both incident disclosure and what is commonly referred to as cyber-hygiene. The incident disclosure component of the Final Rule requires issuers to publicly disclose a material cybersecurity incident on their Form 8–K within four business days following the public company's determination that the incident is material. The cyber-hygiene disclosure obligations pertain to risk management and governance, including disclosures relating to a company's policies and procedures for identifying and managing cybersecurity risks as well as the company's board of director's oversight of cyber risk.

Committee Republicans generally appreciate the SEC's desire to enhance transparency around material disclosures and recognize the increasing risk to issuers from threat actors. However, given that the Commission unanimously approved Guidance on Public Company Cybersecurity Disclosures in 2018, the Commission failed to persuasively articulate why a formal, prescriptive Rule was necessary at this time.

The Rule also continues the SEC's recent trend away from the materiality standard and towards expansive, one-size-fits-all, prescriptive rulemaking covering even non-financial matters. Additionally, the SEC did not sufficiently harmonize the Rule with other state and federal agency rulemaking on this matter. In fact, the SEC concedes that the Cyber Rule's incident disclosure requirements may conflict with certain disclosure requirements from other state and federal laws or other federal agency rulemaking. In such cases, the SEC asserts that either the Cyber Rule would preempt these conflicts or in one specific scenario, the SEC would subsequently modify the Rule to account for them.

Even the minority of commenters that were generally supportive of a prescriptive Rule, such as the North American Securities Administrators Association, Inc. (NASAA), expressed concerns with aspects of the Rule. For example, NASAA wrote that "[they] share the concern expressed by others that the Proposal would not provide for any reporting delay based on an ongoing external investigation related to a cybersecurity incident." As NASAA noted, the

SEC's determination that the need for cybersecurity incident disclosure outweighs law enforcement investigations is problematic. To address this critique, the SEC crafted an overly narrow incident reporting delay in the Final Rule that failed to adequately respond to this serious concern.

Moreover, while Committee Republicans understand the growing cyber risks posed to U.S. public companies and the American economy at large, the SEC may not be the appropriate agency to assess such risk. Additionally, the disclosures required by the Rule fail to adequately mitigate or alleviate a cyber threat and potentially give threat actors a "road map" to inflict greater harm on a given company or industry. This rule could also significantly harm a company's stock price if the information being disclosed is incomplete or inaccurate, resulting in mispriced securities and uninformed market speculation.

While the SEC concluded the Cyber Rule was necessary in part because of concerns that material cybersecurity incidents were underreported, there is at least one independent law firm report indicating a subsequent overreporting of non-material cyber incidents since the Cyber Rule was implemented. If such claims of overreporting are accurate, the disclosures required by the Rule would not provide decision-useful information for investors. Instead, the Rule would merely increase compliance and legal costs that could be better allocated to cybersecurity prevention.

The Cyber Rule is a heavy handed and misplaced approach to the increased threat of cybersecurity incidents. The SEC would have been better served reaching out to industry experts and investors engaging in a dialogue to determine the appropriate course of action. Given that the SEC conceded it may have to modify certain aspects of the Rule if it "becomes appropriate in light of future developments," the Rule should be revoked.

RELATED HEARING

Pursuant to clause 3(c)(6) of rule XIII, the following hearing was used to develop H.J. Res. 100: The Committee on Financial Services held a hearing on April 13, 2023, titled "Oversight of the Securities and Exchange Commission."

COMMITTEE CONSIDERATION

The Committee on Financial Services met in open session on May 16, 2024, and ordered H.J. Res. 100 to be reported favorably to the House by a recorded vote of 27 ayes to 22 nays (Record vote no. FC–152), a quorum being present.

COMMITTEE VOTES

Clause 3(b) of rule XIII of the Rules of the House of Representatives requires the Committee to list the record votes on the order to report legislation and amendments thereto. H.J. Res. 100 was ordered reported favorably to the House by a recorded vote of 27 ayes to 22 nays (Record vote no. FC–152), a quorum being present.

Record vote no. FC - 152

Representative	Yea	Nay	Present
Mr. McHenry	X		
Mr. Hill	X		
Mr. Lucas	X		
Mr. Sessions	X		
Mr. Posey	X		
Mr. Luetkemeyer	X		
Mr. Huizenga	X		
Mrs. Wagner	X		
Mr. Barr	X		
Mr. Williams (TX)	X		
Mr. Emmer			
Mr. Loudermilk	X		
Mr. Mooney	X		
Mr. Davidson	X		
Mr. Rose	X		
Mr. Steil	X		
Mr. Timmons	X		
Mr. Norman	X		
Mr. Meuser	X		
Mr. Fitzgerald	X		
Mr. Garbarino	X		
Mrs. Kim	X		
Mr. Donalds			
Mr. Flood	X		
Mr. Lawler	X		
Mr. Nunn	X		
Ms. De La Cruz	X		
Mrs. Houchin	X		
Mr. Ogles	X		
Ms. Waters		X	
Mrs. Velázquez		X	
Mr. Sherman		X	
Mr. Meeks		X	
Mr. Scott		X	
Mr. Lynch		X	
Mr. Green		X	
Mr. Cleaver			
Mr. Himes		X	
Mr. Foster		X	
Mrs. Beatty		X	
Mr. Vargas		X	
Mr. Gottheimer		X	
Mr. Gonzalez		X	
Mr. Casten		X	
Ms. Pressley		X	
Mr. Horsford		X	
Ms. Tlaib		X	
Mr. Torres		X	
Ms. Garcia		X	
Ms. Williams (GA)		X	
Mr. Nickel		X	
Ms. Pettersen		X	

COMMITTEE OVERSIGHT FINDINGS

Pursuant to clause 3(c) of rule XIII of the Rules of the House of Representatives, the findings and recommendations of the Committee, based on oversight activities under clause 2(b)(1) of rule X of the Rules of the House of Representatives, are incorporated in the descriptive portions of this report.

PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII of the Rules of the House of Representatives, the goal of H.J. Res. 100 is to rescind the SEC's rule relating to "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure."

CONGRESSIONAL BUDGET OFFICE ESTIMATES

Pursuant to clause 3(c)(3) of rule XIII of the Rules of the House of Representatives, the following is the cost estimate provided by the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974:

H.J. Res. 100, a joint resolution providing for congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Securities and Exchange Commission relating to "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure"
As ordered reported by the House Committee on Financial Services on May 16, 2024

By Fiscal Year, Millions of Dollars	2024	2024-2029	2024-2034
Direct Spending (Outlays)	0	0	0
Revenues	0	*	*
Increase or Decrease (-) in the Deficit	0	*	*
Spending Subject to Appropriation (Outlays)	0	*	not estimated

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2035?	No	Statutory pay-as-you-go procedures apply?	Yes
		Mandate Effects	
Increases *on-budget deficits* in any of the four consecutive 10-year periods beginning in 2035?	*	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

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

H.J. Res. 100 would disapprove a final rule published by the Securities and Exchange Commission (SEC) in August 2023.[1] By invoking a legislative process established in the Congressional Review Act, the resolution would repeal the rule and prohibit the agency from issuing the same or any similar rule in the future.

The rule requires public companies that are subject to the SEC's reporting requirements to disclose details about managing and governing risks related to cybersecurity and material incidents. The rule also requires companies to input the information into a structured reporting system.

[1] Securities and Exchange Commission "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosures," Final Rule, 88 *Fed. Reg.* 51896 (August 4, 2023), https://tinyurl.com/mthdwt6x.

CBO estimates that repealing the rule would have an insignificant effect on the SEC's costs. Because the SEC is authorized to collect fees each year to offset its annual appropriation, CBO expects that the net effect on discretionary spending over the 2024–2029 period would be negligible, assuming appropriation actions consistent with that authority.

CBO also expects that repealing the rule could reduce civil monetary penalties that the SEC may seek against individuals and companies that violate the disclosure requirements of the rule. Civil monetary penalties are recorded as revenues in the federal budget. CBO expects that companies would generally comply with the new requirements in that rule and thus any reduction in penalties under the bill would be insignificant over the 2024–2034 period.

The CBO staff contact for this estimate is Aurora Swanson. The estimate was reviewed by H. Samuel Papenfuss, Deputy Director of Budget Analysis.

PHILLIP L. SWAGEL,
Director, Congressional Budget Office.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Pursuant to clause 3(c)(2) of rule XIII of the Rules of the House of Representatives, the Committee adopts as its own the estimate of new budget authority, entitlement authority, or tax expenditures or revenues contained in the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1973.

FEDERAL MANDATES STATEMENT

Pursuant to section 423 of the Unfunded Mandates Reform Act, the Committee adopts as its own the estimate of the Federal mandates prepared by the Director of the Congressional Budget Office.

ADVISORY COMMITTEE STATEMENT

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

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

EARMARK IDENTIFICATION

With respect to clause 9 of rule XXI of the Rules of the House of Representatives, the Committee has carefully reviewed the provisions of the bill and states that the provisions of the bill do not contain any congressional earmarks, limited tax benefits, or limited tariff benefits within the meaning of the rule.

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 the bill establishes or reauthorizes a program of the Federal Govern-

ment known to be duplicative of another Federal program, including any program that was included in a report to Congress pursuant to section 21 of the Public Law 111–139 or the most recent Catalog of Federal Domestic Assistance.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

This Joint Resolution disapproves the rule submitted by the SEC relating to "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" and asserts that such rule shall have no force or effect.

MINORITY VIEWS

This Congressional Review Act ("CRA") resolution would overturn an important SEC rule that provides much needed transparency regarding corporate cybersecurity risks (hereinafter "cybersecurity rule").[1] Specifically, this cybersecurity rule requires SEC-registered public companies to disclose material cybersecurity incidents and information about what they are doing to manage their cyber risks. At a time when cybersecurity risks are increasingly a primary concern of businesses across America, this bill would reduce investors' ability to assess those risks and make more informed decisions about their investment strategies. Moreover, by virtue of this bill being a CRA resolution, it would not only overturn this critical rule, but it would also prevent the SEC from ever issuing a substantially similar rule in the future, which would make it very difficult for the SEC to provide any future guidance or regulation on cybersecurity risks.

The SEC's cybersecurity rule mandates that each public company registered with the SEC provide disclosures in their periodic 8–K filing within four business days of discovering any material cybersecurity breach, as well as to put forth in their annual 10–K disclosures any risk management, strategy, and governance processes they have put in place to mitigate cyber risks. This rule is carefully drafted to balance the needs of both investors and the companies themselves by limiting the disclosures based on the well-known standard of "materiality"—in other words, whether the company thinks that the incident will be of use to its investors when deciding whether or not to trade in the company's shares. This way, investors are kept abreast of any cyber-attacks that might impact a company's operations and market capitalization, while companies are not overly burdened with compliance costs as they do not need to spend time and resources disclosing every single incident, all the way down to the smallest and most insignificant.

The SEC's cyber disclosure rule was put in place in response to a precipitous uptick in the number of cyber-attacks on companies over the last several years, which CEOs and economic experts alike have acknowledged are one of the top threats to their operations and ability to create shareholder value going forward.[2] Recent examples of cybersecurity breaches show just how devastating of an impact these types of incidents can have on public companies, investors, and the U.S. more broadly. For example, in 2021, the largest gas pipeline operator and largest meat processing plant in the

---

[1] SEC Final Rule on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies (Approved July 26, 2023), *available* https://www.sec.gov/news/press-release/2023-139 (17 CFR Parts 229, 232, 239, 240, and 249; Release Nos. 33–11216; 34–97989; File No. S7–09–22).

[2] Better Markets, Letter Submitted to SEC Secretary Vanessa Countryman re: Rule entitled "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure" (File No. S7–09–22, RIN 3235–AM89) (Submitted May 9, 2022).

U.S. were forced to halt operations due to a pair of cyberattacks that cut off 45% of the oil to the East Coast and halted production of a company that provides one-fifth of the U.S.'s meat supply.[3] Additionally, in 2017, the disclosure of a major data breach at credit reporting agency Equifax caused the company's share price to plummet 35%, and insider executives who sold their shares prior to this news becoming public saved themselves millions of dollars in losses while ordinary investors were stuck with the bill.[4] These attacks continue to happen to this day: in November 2023, Russian hackers were able to obtain emails and documents from accounts of Microsoft's senior leadership, cybersecurity, and legal teams;[5] only two months later, hackers accessed the genetic information of nearly 7 million 23andMe users.[6]

As the above incidents make apparent, data breaches and cyberattacks hurt ordinary investors and companies themselves. While many companies already disclose information about their material cybersecurity risks voluntarily, this information is often disjointed, inconsistent, and not comparable.[7] The SEC's cybersecurity rule improves upon the status quo on all fronts, and makes the disclosures much more decision-useful for investors.[8] H.J. Res. 100 harms investors by overturning this critical cybersecurity rule, thereby making it harder for investors to understand cybersecurity risks that have material implications on their investments. Furthermore, as with all CRAs, if H.J. Res. 100 is passed, it would not only overturn the SEC's cybersecurity rule altogether, it would also prevent the SEC from issuing any "substantially similar" rules in the future. This means that the SEC will have very limited options going forward to help investors better understand corporate cybersecurity risks.

This bill is opposed by many prominent investor-centric organizations, including Americans for Financial Reform, Public Citizen, Better Markets, Council of Institutional Investors, the North American Securities Administrators Association Inc. ("NASAA"), and the California Public Employees' Retirement System ("CalPERS").

For these reasons, we oppose H.J. Res. 100.

Sincerely,

MAXINE WATERS,
Ranking Member.
NYDIA M. VELÁZQUEZ,
DAVID SCOTT,
AL GREEN,
Ranking Member, Subcommittee on Oversight and Investigations.
JIM HIMES,

---

[3] *Id.* at 2–3.
[4] Bloomberg, Three Equifax Managers Sold Stock Before Cyber Hack Revealed (Sep. 7, 2017).
[5] The Center for Strategic and International Studies, Significant Cyber Incidents (accessed Jul. 24, 2024).
[6] The Guardian, Genetic testing firm 23andMe admits hackers accessed DNA data of 7m users (Dec. 5, 2023).
[7] SEC, Fact Sheet: Public Company Cybersecurity Disclosures; Final Rules (Jul. 26, 2024) ("Although registrants' disclosures of material cybersecurity incidents and cybersecurity risk management and governance have improved since the 2011 and 2018 [staff] guidance, disclosure practices are inconsistent, necessitating new rules.").
[8] SEC, Fact Sheet: Public Company Cybersecurity Disclosures; Final Rules (Jul. 26, 2024).

JOYCE BEATTY,
SEAN CASTEN,
BRAD SHERMAN,
STEPHEN F. LYNCH,
EMANUEL CLEAVER II,
BILL FOSTER,
JUAN VARGAS,
AYANNA PRESSLEY,
RASHIDA TLAIB,
NIKEMA WILLIAMS,
SYLVIA R. GARCIA,
Members of Congress.

○