

Calendar No. 281

117TH CONGRESS }
2d Session }

SENATE

{ REPORT
{ 117-102

SBA CYBER AWARENESS ACT

MAY 3, 2022.—Ordered to be printed

Mr. CARDIN, from the Committee on Small Business and
Entrepreneurship, submitted the following

R E P O R T

[To accompany H.R. 3462]

[Including cost estimate of the Congressional Budget Office]

The Committee on Small Business and Entrepreneurship, to which was referred the bill (H.R. 3462) to require an annual report on the cybersecurity of the Small Business Administration, and for other purposes, reports favorably thereon, without amendment and recommends that the bill do pass.

I. INTRODUCTION

A bill to require an annual report on the cybersecurity of the SBA and issue additional reports as necessary was introduced by Representatives Jason Crow and Young Lee on May 21, 2021. A Senate companion, S. 1691, was introduced by Senators Marco Rubio, Jim Risch, and Bill Cassidy on May 18, 2021.

This bill requires the Administrator to issue a report within 180 days of enactment, and annually thereafter, to the appropriate Congressional committees (defined in the bill as the Committee on Small Business and Entrepreneurship of the Senate and the Committee on Small Business of the House of Representatives) that includes: (1) an assessment of the information technology (as defined in section 11101 of title 40, United States Code) and cybersecurity infrastructure of the Administration; (2) a strategy to increase the cybersecurity infrastructure of the Administration; (3) a detailed account of any information technology equipment or interconnected system or subsystem of equipment of the Administration that was manufactured by an entity that has its principal place of business located in the People's Republic of China; and (4) an account of any cybersecurity risk or incident that occurred at the Administration

during the 2-year period preceding the date on which the report is submitted, and any action taken by the Administrator to respond to or remediate any such cybersecurity risk or incident.

The bill also requires the SBA to issue additional reports if the Administrator determines that there is a reasonable basis to conclude that a cybersecurity risk or incident occurred at SBA. Specifically, after a cybersecurity risk or incident, the Administrator must notify the appropriate Congressional committees within 7 days and issue a report to those committees containing a summary of the incident and an estimate of the number of small business affected within 30 days. Finally the bill requires the SBA to notify affected small business within 30 days of determining that a cybersecurity risk or incident occurred at the Administration.

The bill was approved by a voice vote as part of a manager's package.

II. HISTORY (PURPOSE & NEED FOR LEGISLATION)

For more than twenty years, SBA's Office of Inspector General has listed IT security as one of the most serious management and performance challenges facing the SBA. The unprecedented demand for COVID 19 relief programs, the Paycheck Protection Program (PPP) and the Economic Injury Disaster Loan (EIDL) programs, inundated the SBA's legacy systems, leading to backend system crashes, portals operating slowly, and a glitch that led to a data breach of applicants' personal information. On March 25, 2020, SBA discovered a flaw in its EIDL application system that exposed the personal information of up to 8,000 individuals to other applicants. Exposed data included email addresses, citizenship status, insurance information, birth dates, phone numbers, addresses, and Social Security Numbers. SBA failed to make any public announcement about the data breach, and it wasn't until April 13, 2020 that the agency sent paper notifications to affected individuals.

III. HEARINGS & ROUNDTABLES

In the 116th Congress the Committee held a hearing entitled "Cyber Crime: An Existential Threat to Small Business" on March 16, 2019. At the hearing, Chairman Rubio highlighted the need for SBA to update its IT systems to prevent a breach and the theft or loss of sensitive small business data, as well as the national security risks of inadequate cybersecurity protections. Chairman Rubio also spoke about his introduction of the "SBA Cyber Awareness Act". Ranking Member Ben Cardin cited that the Office of Inspector General's annual report on major SBA Management and Performance Challenges has identified deficiencies in SBA's IT systems on multiple occasions. Maria Roat, then-SBA CIO, testified about steps the SBA had taken to modernize their IT systems and steps taken to address cybersecurity at the Agency, but stated in her written testimony that 8 of 50 IT management and performance challenge recommendations made by the SBA Office of Inspector General (OIG) remained outstanding. Ranking Member Cardin indicated that Congress needs to be provided updates by SBA on their progress to address IT deficiencies.

IV. DESCRIPTION OF BILL

This bill amends Section 10 of the Small Business Act (15 U.S.C. § 639) by inserting subsection (b) Cybersecurity Reports. The SBA is required to submit an annual report on the cybersecurity infrastructure of the agency to the Small Businesses and Entrepreneurship Committee of the Senate and the Small Business Committee of the House of Representatives in which the Administrator shall, to the maximum extent practicable, include a detailed description of the Administrator's actions taken to respond to or remediate any cybersecurity risk or incident that took place, to include the country of origin of the cybersecurity attack. In the event of a cybersecurity risk or incident, the SBA is required to alert the committees no later than 7 days after the event and submit a report within 30 days. The SBA is also required to provide notice to affected individuals and small business concerns within 30 days.

V. COMMITTEE VOTE

In compliance with rule XXVI (7)(b) of the Standing Rules of the Senate, the following vote was recorded on February 15, 2022.

A motion to adopt H.R. 3462, a bill to require an annual report on the cybersecurity of the Small Business Administration (SBA), was agreed to by a majority voice vote of a quorum present as part of a manager's package.

VI. COST ESTIMATE

In compliance with rule XXVI (11)(a)(1) of the Standing Rules of the Senate, the Committee estimates the cost of the legislation will be equal to the amounts discussed in the following letter from the Congressional Budget Office and available at <https://www.cbo.gov/system/files/2022-02/hr3462.pdf>.

H.R. 3462, SBA Cyber Awareness Act			
As passed by the House of Representatives on November 2, 2021			
By Fiscal Year, Millions of Dollars	2022	2022-2026	2022-2031
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	*	not estimated
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 2032?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No
* = between zero and \$500,000.			

H.R. 3462 would require the Small Business Administration (SBA) to report annually to the Congress on the state of its information technology (IT) and cybersecurity systems, the methods it could use to improve cybersecurity, any of its IT equipment or sys-

tems that were produced by an entity doing business principally in China, and any recent cybersecurity risks or incidents and subsequent responses. The act also would require the SBA to report all cybersecurity risks or incidents to the Congress as they occur and to notify the affected individuals and small businesses.

Under current law, the SBA is required to submit an annual performance report to the Congress that includes information concerning agency cybersecurity efforts. In addition, the Federal Information Security Modernization Act of 2014 requires federal agencies, including the SBA, to report on the effectiveness of their information security policies and practices each year. Although H.R. 3462 would impose new reporting requirements upon the SBA, the work required to fulfill most of those requirements would not be significant because the SBA already collects most of the information needed in those reports.

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

VII. EVALUATION OF REGULATORY IMPACT

In compliance with rule XXVI (11)(b) of the Standing Rules of the Senate, it is the opinion of the Committee that no significant additional regulatory impact will be incurred in carrying out the provisions of this legislation.

VIII. SECTION-BY-SECTION ANALYSIS

Section 1. Short title

This section designates the act as the “SBA Cyber Awareness Act”.

Sec. 2. Cybersecurity awareness reporting

This section amends Section 10 of the Small Business Act (15 U.S.C. § 639) by inserting subsection (b) Cybersecurity Reports. SBA is required to submit an annual report on the cybersecurity infrastructure of the agency to the Small Businesses and Entrepreneurship Committee of the Senate and the Small Business Committee of the House of Representatives. In the event of a cybersecurity risk or incident, SBA is required to alert the committees no later than 7 days after the event and submit a report within 30 days. SBA is also required to provide notice to affected individuals and small business concerns within thirty days.