Calendar No. 217

115TH CONGRESS *1st Session*	SENATE	REPORT 115–153

MAKING AVAILABLE INFORMATION NOW TO STRENGTHEN TRUST AND RESILIENCE AND ENHANCE ENTERPRISE TECHNOLOGY CYBERSECURITY ACT OF 2017

R E P O R T

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ON

S. 770

SEPTEMBER 11, 2017.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

69–019 WASHINGTON : 2017

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

JOHN THUNE, South Dakota, *Chairman*

ROGER F. WICKER, Mississippi	BILL NELSON, Florida
ROY BLUNT, Missouri	MARIA CANTWELL, Washington
TED CRUZ, Texas	AMY KLOBUCHAR, Minnesota
DEB FISCHER, Nebraska	RICHARD BLUMENTHAL, Connecticut
JERRY MORAN, Kansas	BRIAN SCHATZ, Hawaii
DAN SULLIVAN, Alaska	EDWARD J. MARKEY, Massachusetts
DEAN HELLER, Nevada	CORY A. BOOKER, New Jersey
JAMES M. INHOFE, Oklahoma	TOM UDALL, New Mexico
MIKE LEE, Utah	GARY C. PETERS, Michigan
RON JOHNSON, Wisconsin	TAMMY BALDWIN, Wisconsin
SHELLEY MOORE CAPITO, West Virginia	TAMMY DUCKWORTH, Illinois
CORY GARDNER, Colorado	MARGARET WOOD HASSAN, New Hampshire
TODD C. YOUNG, Indiana	CATHERINE CORTEZ MASTO, Nevada

NICK ROSSI, *Staff Director*
ADRIAN ARNAKIS, *Deputy Staff Director*
JASON VAN BEEK, *General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRISTOPHER DAY, *Democratic Deputy Staff Director*

Calendar No. 217

115TH CONGRESS *1st Session* | SENATE | REPORT 115–153

MAKING AVAILABLE INFORMATION NOW TO STRENGTHEN TRUST AND RESILIENCE AND ENHANCE ENTERPRISE TECHNOLOGY CYBERSECURITY ACT OF 2017

SEPTEMBER 11, 2017.—Ordered to be printed

Mr. THUNE, from the Committee on Commerce, Science, and Transportation, submitted the following

R E P O R T

[To accompany S. 770]

[Including cost estimate of the Congressional Budget Office]

The Committee on Commerce, Science, and Transportation, to which was referred the bill (S. 770) to require the Director of the National Institute of Standards and Technology to disseminate resources to help reduce small business cybersecurity risks, and for other purposes, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill (as amended) do pass.

PURPOSE OF THE BILL

S. 770, the Making Available Information Now to Strengthen Trust and Resilience and Enhance Enterprise Technology Cybersecurity Act of 2017 or MAIN STREET Cybersecurity Act of 2017, will improve cybersecurity resources for small businesses. The Act would require the Director of the National Institute of Standards and Technology (NIST Director), under the Department of Commerce, to consider small business concerns and disseminate resources to help small businesses reduce cyber risks by using voluntary risk management security measures as articulated in the public-private initiative, the Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).

BACKGROUND AND NEEDS

According to the Small Business Administration (SBA), small businesses make up more than half of the jobs in the United

States,[1] and they also are a major target for cyber attacks. In the last 5 years, security vendor Symantec Corporation has observed a steady increase in attacks targeting businesses with fewer than 250 employees, with 43 percent of all attacks in 2015 targeted at small businesses.[2]

On December 18, 2014, President Obama signed into law the Cybersecurity Enhancement Act of 2014 (Act of 2014) (15 U.S.C. 7421 et seq.), which then-Committee Chairman Rockefeller and Ranking Member Thune co-authored. That Act amended the NIST Act (15 U.S.C. 271 et seq.) to authorize the NIST Director to work in collaboration with industry on a set of voluntary, consensus-based, and industry-led standards and procedures to reduce cyber risks to critical infrastructure, codifying the process that develops the Cybersecurity Framework.[3] The Cybersecurity Framework is flexible and scalable so that all companies may use it at all organizational levels. Nevertheless, some small companies may need additional resources to make better use of the expansive framework. In addition, several Federal agencies, including the Federal Trade Commission, Department of Homeland Security, and SBA, have issued cybersecurity tips for small businesses that are not coordinated with the Cybersecurity Framework, though they often lay out similar principles.

SUMMARY OF PROVISIONS

S. 770, as amended in Committee, would incorporate NIST consideration of small business concerns into the existing voluntary industry-led process for the Cybersecurity Framework authorized in the Act of 2014. The bill also would direct NIST, in consultation with other relevant agencies, such as the agencies named above, to develop concise, voluntary cybersecurity resources for small businesses in carrying out the Cybersecurity Framework. In addition, the bill would direct other Federal agencies to harmonize, to the extent possible, future cybersecurity resources for small businesses with the resources NIST provides.

LEGISLATIVE HISTORY

On March 29, 2017, Senator Schatz introduced S. 770 with Senators Risch, Thune, Cantwell, Nelson, Gardner, and Cortez Masto as co-sponsors. On April 5, 2017, in an open Executive Session, the Committee considered the bill as modified by a first degree amendment offered by Senator Schatz to improve the bill. The amendment made minor changes to clarify that the resources should apply to a wide range of small businesses and include elements to promote awareness of a workplace cybersecurity culture and third party stakeholder relationships. The Committee, by voice vote, unanimously ordered S. 770 to be reported favorably with an amendment (in the nature of a substitute).

---

[1] Small Business Administration, "Small Business Trends," at https://www.sba.gov/managing-business/running-business/energy-efficiency/sustainable-business-practices/small-business-trends.

[2] Symantec, "Internet Security Threat Report," Volume 21, April 2016, at https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf.

[3] National Institute for Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, February 12, 2014, at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

ESTIMATED COSTS

In accordance with paragraph 11(a) of rule XXVI of the Standing Rules of the Senate and section 403 of the Congressional Budget Act of 1974, the Committee provides the following cost estimate, prepared by the Congressional Budget Office:

S. 770—MAIN STREET Cybersecurity Act of 2017

S. 770 would direct the National Institute of Standards and Technology (NIST) to provide resources to small businesses to help them reduce their cybersecurity risks. Under the bill, NIST would be required to provide and update tools, methodologies, guidelines, and other resources to small business to use on a voluntary basis. Based on an analysis of information from NIST, CBO estimates that implementing S. 770 would cost $6 million over the 2018–2022 period, including $2 million in 2018 for NIST to consult with several federal agencies and develop such resources and an additional $4 million over the 2019–2022 period to update those resources; such spending would be subject to the availability of appropriated funds.

Enacting S. 770 would not affect direct spending or revenues; therefore, pay-as-you-go procedures do not apply. CBO estimates that enacting S. 770 would not increase net direct spending or on-budget deficits in any of the four consecutive 10-year periods beginning in 2028.

S. 770 contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act and would not affect the budgets of state, local, or tribal governments.

The CBO staff contact for this estimate is Stephen Rabent. The estimate was approved by H. Samuel Papenfuss, Deputy Assistant Director for Budget Analysis.

REGULATORY IMPACT STATEMENT

In accordance with paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee provides the following evaluation of the regulatory impact of the legislation, as reported:

NUMBER OF PERSONS COVERED

S. 770, as reported, would develop consistent resources that are fully voluntary for a small business to use. As such, the bill would not create any new programs or impose any new regulatory requirements, and therefore would not subject any individuals or businesses to new regulations.

ECONOMIC IMPACT

S. 770 is not expected to have an adverse impact on the Nation's economy.

PRIVACY

S. 770 is not expected to have an adverse impact on the personal privacy of individuals.

PAPERWORK

S. 770 would not increase paperwork requirements for private individuals or businesses. S. 770 would require the NIST Director to develop and disseminate resources for small businesses to reduce cybersecurity risks.

CONGRESSIONALLY DIRECTED SPENDING

In compliance with paragraph 4(b) of rule XLIV of the Standing Rules of the Senate, the Committee provides that no provisions contained in the bill, as reported, meet the definition of congressionally directed spending items under the rule.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

This section would establish the bill's short title as the "Making Available Information Now to Strengthen Trust and Resilience and Enhance Enterprise Technology Cybersecurity Act of 2017" or the "MAIN STREET Cybersecurity Act of 2017."

Section 2. Findings

This section would present a number of congressional findings. It would find that small businesses are critical to the U.S. economy, accounting for 54 percent of all domestic sales and 55 percent of domestic jobs. This section also would find that small and midsized businesses are major targets for cyberattacks. Additionally, this section would note that the industry-led process authorized by the Act of 2014 continues to play a key role in improving the cyber resilience of the United States. Finally, the section would find that there is a need to develop simplified resources for small businesses that are consistent with the Cybersecurity Framework in order to increase its use.

Section 3. Improving cybersecurity of small businesses

This section would define a number of terms used in the Act. It would amend the NIST Act to ensure the NIST Director considers small business concerns in carrying out the public-private partnership to develop the Cybersecurity Framework authorized in the Act of 2014.

This section would further require that not later than 1 year after the date of enactment of this Act, the NIST Director, in consultation with the heads of other Federal agencies, as the NIST Director considers appropriate, provide clear and concise voluntary resources, such as tips, tools, guidelines, and other ways of providing information, to small businesses to reduce cybersecurity risks. The section would require that NIST ensures that the resources are generally applicable and usable by a wide range of small businesses. In addition, it would require that these resources vary relative to the nature and size of the small business concern and the sensitivity of the data collected or stored.

It would further require the resources be technology-neutral, based on international standards to the extent possible, and consistent with the Stevenson-Wydler Technology Innovation Act of 1980 (15 U.S.C. 3701 et seq.), which seeks to foster government-in-

dustry cooperation. The resources also would include elements that promote awareness of basic controls, a workplace cybersecurity culture, and third party stakeholder relationships. The section also would require NIST to ensure the resources are consistent with the efforts of the National Cybersecurity Awareness and Education Program, otherwise referred to as the NIST National Initiative for Cybersecurity Education, authorized in the Act of 2014. This section also would require NIST to consider any methods included in the Small Business Development Center Cyber Strategy established in the National Defense Authorization Act for Fiscal Year 2017 (Pub. L. 114–328, 130 Stat. 2000).

NIST and such heads of other Federal agencies as the NIST Director considers appropriate would be required to make information on the resources prominently available online in a consistent, clear, and concise manner. Federal agencies publishing additional resources to help small businesses reduce cybersecurity risk after the date of enactment also would be required, to the extent practicable, to make these resources consistent with the resources that NIST provides.

The Committee finds that the public-private partnership to develop the Cybersecurity Framework has been widely lauded. Industry and government have successfully collaborated on voluntarily addressing and managing cybersecurity risks without placing regulatory requirements on businesses. NIST also recognizes in the Cybersecurity Framework that organizations may have unique risks and the use of the framework will vary. As such, the Committee expects NIST to continue its collaboration with industry in carrying out this Act.

Further, the resources developed under this Act should be viewed as voluntary and, thus, would not place additional regulatory requirements on businesses. These resources also are intended to be technology-neutral, consistent with the direction for the process to develop the Cybersecurity Framework. The Committee finds that the principle of tech-neutrality ensures that stakeholders take into account rapid advances and changes in technology. The Committee recognizes that the U.S. technology sector continues to innovate and produce emerging cybersecurity technologies and processes for the marketplace that benefit consumers, small businesses, and the Federal Government. The Committee encourages NIST to consider, in its dissemination of resources, a diverse array of cybersecurity technologies and processes, including the following: multi-factor authentication; data loss prevention; network segmentation; cloud services; data encryption; least privileged architecture; anonymization; software patching and maintenance; and other cybersecurity measures.

CHANGES IN EXISTING LAW

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is enclosed in black brackets, new material is printed in italic, existing law in which no change is proposed is shown in roman):

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY ACT

[31 Stat. 1449]

SEC. 272. ESTABLISHMENT, FUNCTIONS, AND ACTIVITIES.

[15 U.S.C. 272]

* * * * * * *

(e) CYBER RISKS.—

(1) IN GENERAL.—In carrying out the activities under subsection (c)(15), the Director—

(A) shall—

(i) coordinate closely and regularly with relevant private sector personnel and entities, critical infrastructure owners and operators, and other relevant industry organizations, including Sector Coordinating Councils and Information Sharing and Analysis Centers, and incorporate industry expertise;

(ii) consult with the heads of agencies with national security responsibilities, sector-specific agencies and other appropriate agencies, State and local governments, the governments of other nations, and international organizations;

(iii) identify a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, that may be voluntarily adopted by owners and operators of critical infrastructure to help them identify, assess, and manage cyber risks;

(iv) include methodologies—

(I) to identify and mitigate impacts of the cybersecurity measures or controls on business confidentiality; and

(II) to protect individual privacy and civil liberties;

(v) incorporate voluntary consensus standards and industry best practices;

(vi) align with voluntary international standards to the fullest extent possible;

(vii) prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes; [and]

(viii) consider small business concerns (as defined in section 3 of the Small Business Act (15 U.S.C. 632)); and

[(viii)]*(ix)* include such other similar and consistent elements as the Director considers necessary; and

(B) shall not prescribe or otherwise require—

(i) the use of specific solutions;

(ii) the use of specific information or communications technology products or services; or

(iii) that information or communications technology products or services be designed, developed, or manufactured in a particular manner.

(2) LIMITATION.—Information shared with or provided to the Institute for the purpose of the activities described under subsection (c)(15) shall not be used by any Federal, State, tribal, or local department or agency to regulate the activity of any entity. Nothing in this paragraph shall be construed to modify any regulatory requirement to report or submit information to a Federal, State, tribal, or local department or agency.

(3) DEFINITIONS.—In this subsection:

(A) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given the term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c(e)).

(B) SECTOR-SPECIFIC AGENCY.—The term "sector-specific agency" means the Federal department or agency responsible for providing institutional knowledge and specialized expertise as well as leading, facilitating, or supporting the security and resilience programs and associated activities of its designated critical infrastructure sector in the all-hazards environment.

○