PUBLIC LAW 115–236—AUG. 14, 2018

NIST SMALL BUSINESS CYBERSECURITY ACT
Public Law 115–236
115th Congress

An Act

To require the Director of the National Institute of Standards and Technology to disseminate guidance to help reduce small business cybersecurity risks, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "NIST Small Business Cybersecurity Act".

SEC. 2. IMPROVING CYBERSECURITY OF SMALL BUSINESSES.

(a) DEFINITIONS.—In this section:

(1) DIRECTOR.—The term "Director" means the Director of the National Institute of Standards and Technology.

(2) RESOURCES.—The term "resources" means guidelines, tools, best practices, standards, methodologies, and other ways of providing information.

(3) SMALL BUSINESS CONCERN.—The term "small business concern" has the meaning given such term in section 3 of the Small Business Act (15 U.S.C. 632).

(b) SMALL BUSINESS CYBERSECURITY.—Section 2(e)(1)(A) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)(1)(A)) is amended—

(1) in clause (vii), by striking "and" at the end;
(2) by redesignating clause (viii) as clause (ix); and
(3) by inserting after clause (vii) the following:

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

(c) DISSEMINATION OF RESOURCES FOR SMALL BUSINESSES.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Director, in carrying out section 2(e)(1)(A)(viii) of the National Institute of Standards and Technology Act, as added by subsection (b) of this Act, in consultation with the heads of other appropriate Federal agencies, shall disseminate clear and concise resources to help small business concerns identify, assess, manage, and reduce their cybersecurity risks.

(2) REQUIREMENTS.—The Director shall ensure that the resources disseminated pursuant to paragraph (1)—

(A) are generally applicable and usable by a wide range of small business concerns;
(B) vary with the nature and size of the implementing small business concern, and the nature and sensitivity
of the data collected or stored on the information systems
or devices of the implementing small business concern;
(C) include elements, that promote awareness of
simple, basic controls, a workplace cybersecurity culture,
and third-party stakeholder relationships, to assist small
business concerns in mitigating common cybersecurity
risks;
(D) include case studies of practical application;
(E) are technology-neutral and can be implemented
using technologies that are commercial and off-the-shelf;
and
(F) are based on international standards to the extent
possible, and are consistent with the Stevenson-Wydler
(3) NATIONAL CYBERSECURITY AWARENESS AND EDUCATION
PROGRAM.—The Director shall ensure that the resources
disseminated under paragraph (1) are consistent with the
efforts of the Director under section 401 of the Cybersecurity
(4) SMALL BUSINESS DEVELOPMENT CENTER CYBER
STRATEGY.—In carrying out paragraph (1), the Director, to the
extent practicable, shall consider any methods included in the
Small Business Development Center Cyber Strategy developed
under section 1841(a)(3)(B) of the National Defense Authoriza-
tion Act for Fiscal Year 2017 (Public Law 114–328).
(5) VOLUNTARY RESOURCES.—The use of the resources
disseminated under paragraph (1) shall be considered vol-
untary.
(6) UPDATES.—The Director shall review and, if necessary,
update the resources disseminated under paragraph (1) in
accordance with the requirements under paragraph (2).
(7) PUBLIC AVAILABILITY.—The Director and the head of
each Federal agency that so elects shall make prominently
available on the respective agency’s public Internet website
information about the resources and updates to the resources
disseminated under paragraph (1). The Director and the heads
shall each ensure that the information they respectively make
prominently available is consistent, clear, and concise.
(d) OTHER FEDERAL CYBERSECURITY REQUIREMENTS.—Nothing
in this section may be construed to supersede, alter, or otherwise
affect any cybersecurity requirements applicable to Federal agen-
cies.
(e) **Funding.**—This Act shall be carried out using funds otherwise authorized to be appropriated or made available to the National Institute of Standards and Technology.

Approved August 14, 2018.