To provide for the identification and documentation of best practices for cyber hygiene by the National Institute of Standards and Technology, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 29, 2017

Mr. HATCH (for himself and Mr. MARKEY) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To provide for the identification and documentation of best practices for cyber hygiene by the National Institute of Standards and Technology, and for other purposes.

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

SECTION 1. SHORT TITLE.

This Act may be cited as the “Promoting Good Cyber Hygiene Act of 2017”.

SEC. 2. CYBER HYGIENE BEST PRACTICES.

(a) ESTABLISHMENT.—Not later than 1 year after the date of enactment of this Act, the Director of the National Institute of Standards and Technology shall estab-
lish a list of best practices for effective and usable cyber
hygiene—

(1) in consultation with the Federal Trade
Commission and the Secretary of Homeland Secu-

rity;

(2) after notice and an opportunity for public
comment; and

(3) for use by—

(A) the Federal Government;

(B) the private sector; and

(C) any person utilizing an information

system or device.

(b) BEST PRACTICES.—A best practice on the list es-
tablished under subsection (a) shall—

(1) be a simple, basic control that has the
greatest effect in defending against a common cyber-

security threat or risk;

(2) utilize a technology that is commercial, off-

the-shelf, and based on international standards; and

(3) to the degree practicable, be based on and
consistent with the Cybersecurity Framework con-
tained in Executive Order 13636, entitled “Improv-
ing Critical Infrastructure Cybersecurity”, issued in
February 2013, or any successor framework.
(c) VOLUNTARY PRACTICES.—A best practice on the list established under subsection (a) shall be considered voluntary and is not intended to be construed as mandatory.

(d) BASELINE.—The Director shall encourage the use of the best practices as the baseline provided by the list established under subsection (a) is encouraged to be not only used but improved upon by any entity including—

(1) the Federal Government;

(2) the private sector; and

(3) any person utilizing an information system or device.

(e) ANNUAL UPDATES.—Not less frequently than once each year, the Director shall review and update the list established under subsection (a).

(f) PUBLIC AVAILABILITY.—

(1) IN GENERAL.—The Director shall publish the list of best practices established under subsection (a) in a clear and concise format.

(2) AVAILABILITY.—The Federal Trade Commission and the Small Business Administration shall make such list of best practices prominently available on the public Internet website of each respective agency.
(g) Other Federal Cybersecurity Requirements.—Nothing in this section shall be construed to supersede, alter, or otherwise affect any cybersecurity requirements applicable to any Federal agency.

(h) Considerations.—In carrying out subsection (a), the head of each agency of the Federal Government shall consider the benefit, as pertaining to cyber hygiene, of an emerging technology or process capable of providing any enhanced security protection, including—

(1) multi-factor authentication;

(2) data loss prevention;

(3) micro-segmentation;

(4) data encryption;

(5) cloud services;

(6) anonymization;

(7) software patching and maintenance;

(8) phishing education; and

(9) other standard cybersecurity measures to achieve trusted security in the infrastructure.

(i) Study on Emerging Concepts To Promote Effective Cyber Hygiene for the Internet of Things.—

(1) Internet of Things Defined.—The term “Internet of Things” means the set of physical ob-
jects embedded with sensors or actuators and con-
nected to a network.

(2) STUDY REQUIRED.—The Secretary of
Homeland Security, in coordination with the Direc-
tor of the National Institute of Standards and Tech-
nology and the Federal Trade Commission, shall
conduct a study on cybersecurity threats relating to
the Internet of Things.

(3) MATTERS STUDIED.—As part of the study
required by paragraph (2), the Secretary shall—

(A) assess cybersecurity threats relating to
the Internet of Things;

(B) assess the effect such threats may
have on the cybersecurity of the information
systems and networks of the Federal Govern-
ment (except for the information systems and
networks of the Department of Defense and the
intelligence community (as defined in Section 3
of the National Security Act of 1947 (50
U.S.C. 3003))); and

(C) develop recommendations for address-
ing such threats.

(4) REPORT TO CONGRESS.—Not later than 1
year after the date of the enactment of this Act, the
Secretary shall—
(A) complete the study required by paragraph (2); and

(B) submit to Congress a report that contains the findings of the Secretary with respect to such study and the recommendations developed by the secretary under paragraph (3)(C).