

115TH CONGRESS
1ST SESSION

S. 1475

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.

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

3 **SECTION 1. SHORT TITLE.**

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

6 **SEC. 2. CYBER HYGIENE BEST PRACTICES.**

7 (a) ESTABLISHMENT.—Not later than 1 year after
8 the date of enactment of this Act, the Director of the Na-
9 tional 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 Security;

(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 established under subsection (a) shall—

(1) be a simple, basic control that has the greatest effect in defending against a common cybersecurity 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 contained in Executive Order 13636, entitled “Improving Critical Infrastructure Cybersecurity”, issued in February 2013, or any successor framework.

1 (c) VOLUNTARY PRACTICES.—A best practice on the
2 list established under subsection (a) shall be considered
3 voluntary and is not intended to be construed as manda-
4 tory.

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

9 (1) the Federal Government;

10 (2) the private sector; and

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

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

16 (f) PUBLIC AVAILABILITY.—

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

20 (2) AVAILABILITY.—The Federal Trade Com-
21 mission and the Small Business Administration shall
22 make such list of best practices prominently avail-
23 able on the public Internet website of each respective
24 agency.

1 (g) OTHER FEDERAL CYBERSECURITY REQUIRE-
 2 MENTS.—Nothing in this section shall be construed to su-
 3 persede, alter, or otherwise affect any cybersecurity re-
 4 quirements applicable to any Federal agency.

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

- 10 (1) multi-factor authentication;
- 11 (2) data loss prevention;
- 12 (3) micro-segmentation;
- 13 (4) data encryption;
- 14 (5) cloud services;
- 15 (6) anonymization;
- 16 (7) software patching and maintenance;
- 17 (8) phishing education; and
- 18 (9) other standard cybersecurity measures to
 19 achieve trusted security in the infrastructure.

20 (i) STUDY ON EMERGING CONCEPTS TO PROMOTE
 21 EFFECTIVE CYBER HYGIENE FOR THE INTERNET OF
 22 THINGS.—

23 (1) INTERNET OF THINGS DEFINED.—The term
 24 “Internet of Things” means the set of physical ob-

1 jects embedded with sensors or actuators and con-
2 nected to a network.

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

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

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

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

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

23 (4) REPORT TO CONGRESS.—Not later than 1
24 year after the date of the enactment of this Act, the
25 Secretary shall—

1 (A) complete the study required by para-
2 graph (2); and

3 (B) submit to Congress a report that con-
4 tains the findings of the Secretary with respect
5 to such study and the recommendations devel-
6 oped by the secretary under paragraph (3)(C).

○