

.....  
(Original Signature of Member)

115TH CONGRESS  
1ST SESSION

**H. R.** \_\_\_\_\_

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 HOUSE OF REPRESENTATIVES

Ms. ESHOO introduced the following bill; which was referred to the Committee  
on \_\_\_\_\_  
\_\_\_\_\_

**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 National Institute

1 of Standards and Technology, in consultation with the  
2 Federal Trade Commission and the Department of Home-  
3 land Security, after notice and an opportunity for public  
4 comment, shall establish a list of best practices for effec-  
5 tive and usable cyber hygiene for use by the Federal Gov-  
6 ernment, the private sector, and any individual or organi-  
7 zation utilizing an information system or device. Such list  
8 shall—

9 (1) be a list of simple, basic controls that have  
10 the most impact in defending against common  
11 cybersecurity threats and risks;

12 (2) utilize technologies that are commercial off-  
13 the-shelf and based on international standards; and

14 (3) to the degree practicable, be based on and  
15 consistent with the Cybersecurity Framework con-  
16 tained in Executive Order 13636, entitled Improving  
17 Critical Infrastructure Cybersecurity, issued in Feb-  
18 ruary 2013, or any successor framework.

19 (b) VOLUNTARY PRACTICES.—The best practices on  
20 the list established under this section shall be considered  
21 voluntary and are not intended to be construed as a list  
22 of mandatory actions.

23 (c) BASELINE.—The best practices on the list estab-  
24 lished under this section are intended as a baseline for  
25 the Federal Government, the private sector, and any indi-

1 vidual or organization utilizing an information system or  
2 device. Such entities are encouraged to use and improve  
3 on those best practices.

4 (d) UPDATES.—The National Institute of Standards  
5 and Technology shall review and update the list of best  
6 practices established under this section on an annual  
7 basis.

8 (e) PUBLIC AVAILABILITY.—The list of best practices  
9 established under this section shall be published in a clear  
10 and concise format and made available prominently on the  
11 public websites of the Federal Trade Commission and the  
12 Small Business Administration.

13 (f) OTHER FEDERAL CYBERSECURITY REQUIRE-  
14 MENTS.—Nothing in this section shall be construed to su-  
15 percede, alter, or otherwise affect any cybersecurity re-  
16 quirements applicable to Federal agencies.

17 (g) CONSIDERATIONS.—In carrying out subsection  
18 (a), the agencies shall consider the benefits, as they per-  
19 tain to cyber hygiene, of emerging technologies and proc-  
20 esses that provide enhanced security protections, including  
21 multi-factor authentication, data loss prevention, micro-  
22 segmentation, data encryption, cloud services,  
23 anonymization, software patching and maintenance,  
24 phishing education, and other standard cybersecurity  
25 measures to achieve trusted security in the infrastructure.

1 (h) STUDY ON EMERGING CONCEPTS TO PROMOTE  
2 EFFECTIVE CYBER HYGIENE FOR THE INTERNET OF  
3 THINGS.—

4 (1) INTERNET OF THINGS DEFINED.—In this  
5 subsection, the term “Internet of Things” means the  
6 set of physical objects embedded with sensors or ac-  
7 tuators and connected to a network.

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

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

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

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

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

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

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

8                   (B) submit to Congress a report that con-  
9                   tains the findings of such study and the rec-  
10                  ommendations developed.