

.....
(Original Signature of Member)

114TH 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 2015”.

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) be based on the Cybersecurity Framework
15 contained in Executive Order 13636, entitled Im-
16 proving Critical Infrastructure Cybersecurity, issued
17 in February 2013.

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

22 (c) **BASELINE.**—The best practices on the list estab-
23 lished under this section are intended as a baseline for
24 the Federal Government, the private sector, and any indi-
25 vidual or organization utilizing an information system or

1 device. Such entities are encouraged to use and improve
2 on those best practices.

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

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

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

16 (g) EMERGING CONCEPTS TO PROVIDE EFFECTIVE
17 CYBER HYGIENE.—

18 (1) STUDY.—The Secretary of Homeland Secu-
19 rity, in coordination with the National Institute of
20 Standards and Technology and the Federal Trade
21 Commission, shall conduct a study on cybersecurity
22 threats relating to mobile devices.

23 (2) MATTERS STUDIED.—As part of the study
24 required under this subsection, the Secretary shall—

1 (A) assess threats relating to mobile de-
2 vices;

3 (B) assess the effect such threats may
4 have on the cybersecurity of the information
5 systems and networks of the Federal Govern-
6 ment (except for the information systems and
7 networks of the Department of Defense and the
8 Intelligence Community); and

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

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

14 (A) complete the study under this sub-
15 section; and

16 (B) submit a report to Congress that con-
17 tains the findings of such study and the rec-
18 ommendations developed.

19 (h) DEFINITION.—In this section, the term “cyber
20 hygiene” means processes, procedures, and mechanisms
21 that help protect information systems or devices against
22 cybersecurity threats, including—

23 (1) unauthorized access;

- 1 (2) alteration of information or code running or
- 2 intended to be running on such systems or devices;
- 3 and
- 4 (3) unauthorized denials of service to author-
- 5 ized users of these systems or devices.