H. R. 3010

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

JUNE 22, 2017

Ms. ESHOO (for herself and Mrs. BROOKS of Indiana) introduced the following bill; which was referred to the Committee on Science, Space, and Technology:

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 Representatives 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 National Institute of Standards and Technology, in consultation with the
Federal Trade Commission and the Department of Homeland Security, after notice and an opportunity for public comment, shall establish a list of best practices for effective and usable cyber hygiene for use by the Federal Government, the private sector, and any individual or organization utilizing an information system or device. Such list shall—

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

(2) utilize technologies that are 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.

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

(c) BASELINE.—The best practices on the list established under this section are intended as a baseline for the Federal Government, the private sector, and any individual or organization utilizing an information system or
device. Such entities are encouraged to use and improve on those best practices.

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

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

(f) Other Federal Cybersecurity Requirements.—Nothing in this section shall be construed to supersede, alter, or otherwise affect any cybersecurity requirements applicable to Federal agencies.

(g) Considerations.—In carrying out subsection (a), the agencies shall consider the benefits, as they pertain to cyber hygiene, of emerging technologies and processes that provide enhanced security protections, including multi-factor authentication, data loss prevention, micro-segmentation, data encryption, cloud services, anonymization, software patching and maintenance, phishing education, and other standard cybersecurity measures to achieve trusted security in the infrastructure.
(h) Study on Emerging Concepts To Promote Effective Cyber Hygiene for the Internet of Things.—

(1) Internet of Things Defined.—In this subsection, the term “Internet of Things” means the set of physical objects embedded with sensors or actuators and connected to a network.

(2) Study Required.—The Secretary of Homeland Security, in coordination with the Director of the National Institute of Standards and Technology 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 Government (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 addressing 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 such study and the recommendations developed.