Klobuchar-Thune Substitute

Amy Klobuchar

AMENDMENT NO._____ Calendar No._____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—118th Cong., 1st Sess.

S. 2201

To increase knowledge and awareness of best practices to reduce cybersecurity risks in the United States.

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by Ms. KLOBUCHAR

Viz:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "American Cybersecurity Literacy Act".

SEC. 2. CYBERSECURITY LITERACY CAMPAIGN.

(a) IN GENERAL.—The Director of the National Institute of Standards and Technology shall, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, develop and conduct a cybersecurity literacy campaign described in subsection (b), which the Director of the National Institute of Standards and Tech-

nology shall make available in multiple languages and formats, if practicable, to increase the knowledge and awareness of citizens of the United States of best practices to reduce cybersecurity risks.

(b) ELEMENTS.—In carrying out subsection (a), the Director of the National Institute of Science and Technology, in consultation with the Director of the Cybersecurity and Infrastructure Security Agency, shall—

(1) educate citizens of the United States with respect to how to prevent and mitigate a cyberattack or cybersecurity risk, including by—

(A) instructing citizens of the United States with respect to how to identify—

(i) a phishing email or message; and

(ii) a secure website;

(B) instructing citizens of the United States about the benefits of changing default passwords on any hardware or software technology;

(C) encouraging the use of cybersecurity tools, including—

(i) multi-factor authentication;

(ii) a complex password;

(iii) anti-virus software;

(iv) patching or updating software and applications; and

(v) a virtual private network;

(D) identifying a device that could pose possible cybersecurity risks, including—

(i) a personal computer;

(ii) a smartphone;

(iii) a tablet;

(iv) a Wi-Fi router;

(v) a smart home appliance;

(vi) a webcam;

(vii) an internet-connected monitor; or

(viii) any other device that can be connected to the internet, including any mobile device other than a smartphone or tablet;

(E) encouraging citizens of the United States to—

(i) regularly review mobile application permissions;

(ii) decline any privilege request from a mobile application that is unnecessary;

(iii) download an application only from a trusted vendor or source; and

(iv) consider the life cycle of a product and the commitment of a developer to providing security updates during the expected period of use of a connected device; and

(F) identifying any potential cybersecurity risk related to using a publicly available Wi-Fi network and any method a user may use to limit such risks; and

(2) encourage citizens of the United States to use any resource that is developed as a result of this literacy campaign to help mitigate the cybersecurity risks described in this subsection.