Klobuchar-Thune Substitute

AMENDMENT NO._____ Calendar No._____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—117th Cong., 1st Sess.

S. 2699

To establish a cybersecurity literacy campaign, and for other purposes.

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 of 2021".

SEC. 2. SENSE OF CONGRESS.

It is the sense of the Congress that the United States has a national security and economic interest in promoting cybersecurity literacy amongst the general public.

SEC. 3. ESTABLISHMENT OF 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 of the Department of Homeland Security, develop and conduct a cybersecurity literacy campaign to increase the knowledge and awareness of people in the United States of best practices to reduce cybersecurity risks.

(b) ELEMENTS.—In carrying out subsection (a), the Director of the Institute shall—

(1) identify the critical areas of an information technology system that presents cybersecurity risks and educate people in the United States on how to prevent and mitigate such risks by—

(A) instructing such people on how to identify—

(i) phishing emails; and

(ii) secure websites;

(B) instructing such people on the need to change default passwords on hardware and software technology;

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

(i) multi-factor authentication;

(ii) complex passwords;

(iii) firewalls; and

(iv) anti-virus software;

(D) identifying the devices that could pose possible cybersecurity risks, including—

(i) personal computers;

(ii) smartphones;

(iii) tablets;

(iv) Wi-Fi routers; and

(v) smart home appliances;

(E) encouraging such people to—

(i) regularly review mobile application permissions;

(ii) decline privilege requests from mobile applications that are unnecessary;

(iii) download applications only from trusted vendors or sources; and

(iv) connect internet of things or devices to a separate and dedicated network; and

(F) identifying the potential cybersecurity risks of using publicly available Wi-Fi networks and the methods a user may utilize to limit such risks; and

(2) direct people and businesses in the United States to Federal resources to help mitigate the cybersecurity risks identified in this subsection.