H. R. 4055

[Report No. 117–]

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

IN THE HOUSE OF REPRESENTATIVES

JUNE 22, 2021

Mr. KINZINGER (for himself, Mr. BILIRAKIS, Ms. ESHOO, Mr. VEASEY, and Ms. HOULAHAN) introduced the following bill; which was referred to the Committee on Energy and Commerce

AUGUST --, 2021

Reported with an amendment, committed to the Committee of the Whole House on the State of the Union, and ordered to be printed

[Strike out all after the enacting clause and insert the part printed in italic]

[For text of introduced bill, see copy of bill as introduced on June 22, 2021]
A BILL

To establish a cybersecurity literacy campaign, 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 “American Cybersecurity Literacy Act”.

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 Assistant Secretary shall develop and conduct a cybersecurity literacy campaign (which shall be available in multiple languages and formats, if practicable) to increase the knowledge and awareness of the American people of best practices to reduce cybersecurity risks.

(b) Campaign.—To reduce cybersecurity risks, the Assistant Secretary shall—

(1) educate the American people on how to prevent and mitigate cyberattacks and cybersecurity risks, including by—

(A) instructing the American people on how to identify—

(i) phishing emails and messages; and
(ii) secure websites;

(B) instructing the American people about

the benefits of changing default passwords on

hardware and software technology;

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

(i) multi-factor authentication;

(ii) complex passwords;

(iii) anti-virus software;

(iv) patching and updating software

and applications; and

(v) virtual private networks;

(D) identifying the devices that could pose

possible cybersecurity risks, including—

(i) personal computers;

(ii) smartphones;

(iii) tablets;

(iv) Wi-Fi routers;

(v) smart home appliances;

(vi) webcams;

(vii) internet-connected monitors; and

(viii) any other device that can be con-
nected to the internet, including mobile de-

vices other than smartphones and tablets;

(E) encouraging Americans to—
(i) regularly review mobile application
permissions;

(ii) decline privilege requests from mo-
ibile applications that are unnecessary;

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

(iv) consider a product’s life cycle and
the developer or manufacturer’s commit-
ment to providing security updates during
a connected device’s expected period of use;

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) encourage the American people to use re-
sources to help mitigate the cybersecurity risks identi-
fied in this subsection.

(c) ASSISTANT SECRETARY DEFINED.—In this section,
the term “Assistant Secretary” means the Assistant Sec-
retary of Commerce for Communications and Information.