AMENDMENT TO RULES COMMITTEE PRINT FOR
H.R. 6395
OFFERED BY MS. ESHOO OF CALIFORNIA

Add at the end of subtitle C of title XVI the following:

SEC. 16. IMPROVING CYBERSECURITY OF SMALL ORGANIZATIONS.

(a) DEFINITIONS.—In this section:

(1) ADMINISTRATION.—The term “Administration” means the Small Business Administration.

(2) ADMINISTRATOR.—The term “Administrator” means the Administrator of the Administration.

(3) COMMISSION.—The term “Commission” means the Federal Trade Commission.

(4) CYBERSECURITY GUIDANCE.—The term “cybersecurity guidance” means the cybersecurity guidance documented and promoted in the resource maintained under section 3(a).

(5) DIRECTOR.—The term “Director” means the Director of the Cybersecurity and Infrastructure Security Agency.
(6) NIST.—The term “NIST” means the National Institute of Standards and Technology.

(7) SECRETARY.—The term “Secretary” means the Secretary of Commerce.

(8) SMALL BUSINESS.—The term “small business” has the meaning given the term “small business concern” under section 3 of the Small Business Act (15 U.S.C. 632).

(9) SMALL BUSINESS DEVELOPMENT CENTER.—The term “small business development center” has the meaning given the term in section 3 of the Small Business Act (15 U.S.C. 632).

(10) SMALL BUSINESS LENDING COMPANY.—The term “small business lending company” has the meaning given the term in section 3 of the Small Business Act (15 U.S.C. 632).

(11) SMALL GOVERNMENTAL JURISDICTION.—The term “small governmental jurisdiction” has the meaning given the term in section 601 of title 5, United States Code.

(12) SMALL NONPROFIT.—The term “small nonprofit” has the meaning given the term “small organization” in section 601 of title 5, United States Code.
(13) SMALL ORGANIZATION.—The term “small organization” means an organization that is unlikely to employ a specialist in cybersecurity, including—
   (A) a small business;
   (B) a small nonprofit; and
   (C) a small governmental jurisdiction.

(b) CYBERSECURITY GUIDANCE.—
   (1) IN GENERAL.—The Director shall maintain cybersecurity guidance that documents and promotes evidence-based cybersecurity policies and controls for use by small organizations, which shall—
      (A) include simple, basic controls that have the most impact in protecting small organizations against common cybersecurity threats and risks;
      (B) include guidance to address common cybersecurity threats and risks posed by electronic devices that are personal to the employees and contractors of small organizations, as well as electronic devices that are issued to those employees and contractors by small organizations; and
      (C) recommend—
         (i) types of commercial, off-the-shelf technology products and services that im-
prove the cybersecurity of small organizations; and

(ii) configurations and settings for
some of the most commonly used software
that can improve the cybersecurity of small
organizations.

(2) Consistency.—The Director shall ensure
the cybersecurity guidance maintained under para-
graph (1) is consistent with—

(A) cybersecurity resources developed by
NIST, as required by the NIST Small Business
Cybersecurity Act (Public Law 115–236); and

(B) the most recent version of the Cyberse-
curity Framework, or successor resource, main-
tained by NIST.

(3) Updates.—

(A) In General.—The Director shall re-
view the cybersecurity guidance maintained
under paragraph (1) not less frequently than
annually and update as appropriate.

(B) Consultation.—In updating the cy-
bersecurity guidance under subparagraph (A),
the Director shall, to the degree practicable and
as appropriate, consult with—
(i) the Administrator, the Secretary, and the Commission; and

(ii) small organizations, insurers, State governments, companies that work with small organizations, and academic and Federal and non-Federal experts in cybersecurity.

(4) USER INTERFACE.—As appropriate, the Director shall consult with experts regarding the design of a user interface for the cybersecurity guidance.

(c) PROMOTION OF CYBERSECURITY GUIDANCE FOR SMALL BUSINESSES.—

(1) PUBLIC AVAILABILITY.—The cybersecurity guidance maintained under subsection (b)(1) shall be—

(A) made available, prominently and free of charge, on the public website of the Cybersecurity Infrastructure Security Agency; and

(B) linked to from relevant portions of the websites of the Administration and the Minority Business Development Agency.

(2) PROMOTION GENERALLY.—The Director, the Administrator, and the Secretary shall, to the degree practicable, promote the cybersecurity guid-
ance through relevant resources that are intended
for or known to be regularly used by small organiza-
tions, including agency documents, websites, and
events.

(3) PROMOTION AMONG RECIPIENTS OF SBA AS-
SISTANCE.—Not later than one year after the date
of enactment of this Act, the Administrator shall—

(A) encourage the adoption of the cyberse-
curity guidance for small businesses that receive
assistance from the Administration, including
by requiring a brief description of how a small
business will adopt the cybersecurity guidance
or has instituted alternative practices or proce-
dures that meet or exceed the intended out-
comes of the cybersecurity guidance; and

(B) require entities that receive financial
support from the Administration for the pur-
poses of funding or supporting small businesses,
including small business lending companies and
small business development centers, to encour-
age small businesses that work with such enti-
ties to adopt the cybersecurity guidance.

(4) PROMOTION AMONG RECIPIENTS OF MBDA
ASSISTANCE.—Not later than 180 days after the
date of enactment of this Act, the Secretary shall
encourage the adoption of the cybersecurity guidance for small organizations that receive assistance from the Minority Business Development Agency, including by requiring a brief description of how a small organization will adopt the cybersecurity guidance or has instituted alternative practices or procedures that meet or exceed the intended outcomes of the cybersecurity guidance.

(5) RULE OF CONSTRUCTION.—Nothing in paragraphs (3) or (4) may be construed to require adoption of the cybersecurity guidance as a condition of receiving assistance from the Administration or the Minority Business Development Agency.

(d) REPORT ON INCENTIVIZING CYBERSECURITY FOR SMALL ORGANIZATIONS.—

(1) IN GENERAL.—Not later than one year after the date of the enactment of this Act, the Director shall submit to Congress a report describing methods to incentivize small organizations to improve their cybersecurity, including through the adoption of policies, controls, products and services that have been demonstrated to reduce cybersecurity risk.

(2) MATTERS TO BE INCLUDED.—The report required under paragraph (1) shall—
(A) identify barriers or challenges for small organizations in purchasing or acquiring products and services that promote the cybersecurity;

(B) assess market availability, market pricing, and affordability of products and services that promote the cybersecurity for small organizations, with particular attention to identifying high-risk and underserved sectors or regions;

(C) estimate the cost of tax breaks, grants, subsidies, or other incentives to increase the adoption of policies and controls or acquisition of products and services that promote the cybersecurity, for small organizations;

(D) as practicable, consult the certifications and requirement for cloud services described in the final report of the Cyberspace Solarium Commission established under section 1652 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Public Law 115–232; 132 Stat. 2140);

(E) describe evidence-based cybersecurity controls and policies that improve cybersecurity for small organizations; and
(F) with respect to the incentives described in subparagraph (C), recommend measures that can effectively improve cybersecurity at scale for small organizations.

(3) CONSULTATION.—In preparing the report required under paragraph (1), the Director shall consult with—

(A) the Administrator, the Secretary, and the Commission; and

(B) small organizations, insurers, State governments, companies that work with small organizations, and academic and Federal and non-Federal experts in cybersecurity.

(e) PERIODIC CENSUS ON STATE OF CYBERSECURITY OF SMALL BUSINESSES.—

(1) IN GENERAL.—Not later than one year after the date of enactment of this Act and not less frequently than annually thereafter, the Administrator shall submit to Congress and make publicly available data on the state of cybersecurity of small businesses, including—

(A) adoption of the cybersecurity guidance among small businesses;

(B) the most significant cybersecurity vulnerabilities facing small businesses;
(C) the most common challenges facing small businesses in adopting the cybersecurity guidance;

(D) the amount small businesses spend on cybersecurity products and services; and

(E) the personnel small businesses dedicate to cybersecurity (including the amount of total personnel time, whether by employees or contractors, dedicated to cybersecurity efforts).

(2) FORM.—The report required under paragraph (1) shall be produced in unclassified form but may contain a classified annex.