

**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:

1 **SEC. 16__ . IMPROVING CYBERSECURITY OF SMALL ORGA-**
2 **NIZATIONS.**

3 (a) **DEFINITIONS.**—In this section:

4 (1) **ADMINISTRATION.**—The term “Administra-
5 tion” means the Small Business Administration.

6 (2) **ADMINISTRATOR.**—The term “Adminis-
7 trator” means the Administrator of the Administra-
8 tion.

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

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

15 (5) **DIRECTOR.**—The term “Director” means
16 the Director of the Cybersecurity and Infrastructure
17 Security Agency.

1 (6) NIST.—The term “NIST” means the Na-
2 tional Institute of Standards and Technology.

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

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

9 (9) SMALL BUSINESS DEVELOPMENT CEN-
10 TER.—The term “small business development cen-
11 ter” has the meaning given the term in section 3 of
12 the Small Business Act (15 U.S.C. 632).

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

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

21 (12) SMALL NONPROFIT.—The term “small
22 nonprofit” has the meaning given the term “small
23 organization” in section 601 of title 5, United States
24 Code.

1 (13) SMALL ORGANIZATION.—The term “small
2 organization” means an organization that is unlikely
3 to employ a specialist in cybersecurity, including—

4 (A) a small business;

5 (B) a small nonprofit; and

6 (C) a small governmental jurisdiction.

7 (b) CYBERSECURITY GUIDANCE.—

8 (1) IN GENERAL.—The Director shall maintain
9 cybersecurity guidance that documents and promotes
10 evidence-based cybersecurity policies and controls for
11 use by small organizations, which shall—

12 (A) include simple, basic controls that have
13 the most impact in protecting small organiza-
14 tions against common cybersecurity threats and
15 risks;

16 (B) include guidance to address common
17 cybersecurity threats and risks posed by elec-
18 tronic devices that are personal to the employ-
19 ees and contractors of small organizations, as
20 well as electronic devices that are issued to
21 those employees and contractors by small orga-
22 nizations; and

23 (C) recommend—

24 (i) types of commercial, off-the-shelf
25 technology products and services that im-

1 prove the cybersecurity of small organiza-
2 tions; and

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

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

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

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

16 (3) UPDATES.—

17 (A) IN GENERAL.—The Director shall re-
18 view the cybersecurity guidance maintained
19 under paragraph (1) not less frequently than
20 annually and update as appropriate.

21 (B) CONSULTATION.—In updating the cy-
22 bersecurity guidance under subparagraph (A),
23 the Director shall, to the degree practicable and
24 as appropriate, consult with—

1 (i) the Administrator, the Secretary,
2 and the Commission; and

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

8 (4) USER INTERFACE.—As appropriate, the Di-
9 rector shall consult with experts regarding the de-
10 sign of a user interface for the cybersecurity guid-
11 ance.

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

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

17 (A) made available, prominently and free
18 of charge, on the public website of the Cyberse-
19 curity Infrastructure Security Agency; and

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

23 (2) PROMOTION GENERALLY.—The Director,
24 the Administrator, and the Secretary shall, to the
25 degree practicable, promote the cybersecurity guid-

1 ance through relevant resources that are intended
2 for or known to be regularly used by small organiza-
3 tions, including agency documents, websites, and
4 events.

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

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

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

23 (4) PROMOTION AMONG RECIPIENTS OF MBDA
24 ASSISTANCE.—Not later than 180 days after the
25 date of enactment of this Act, the Secretary shall

1 encourage the adoption of the cybersecurity guidance
2 for small organizations that receive assistance from
3 the Minority Business Development Agency, includ-
4 ing by requiring a brief description of how a small
5 organization will adopt the cybersecurity guidance or
6 has instituted alternative practices or procedures
7 that meet or exceed the intended outcomes of the cy-
8 bersecurity guidance.

9 (5) RULE OF CONSTRUCTION.—Nothing in
10 paragraphs (3) or (4) may be construed to require
11 adoption of the cybersecurity guidance as a condi-
12 tion of receiving assistance from the Administration
13 or the Minority Business Development Agency.

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

16 (1) IN GENERAL.—Not later than one year
17 after the date of the enactment of this Act, the Di-
18 rector shall submit to Congress a report describing
19 methods to incentivize small organizations to im-
20 prove their cybersecurity, including through the
21 adoption of policies, controls, products and services
22 that have been demonstrated to reduce cybersecurity
23 risk.

24 (2) MATTERS TO BE INCLUDED.—The report
25 required under paragraph (1) shall—

1 (A) identify barriers or challenges for
2 small organizations in purchasing or acquiring
3 products and services that promote the cyberse-
4 curity;

5 (B) assess market availability, market prie-
6 ing, and affordability of products and services
7 that promote the cybersecurity for small organi-
8 zations, with particular attention to identifying
9 high-risk and underserved sectors or regions;

10 (C) estimate the cost of tax breaks, grants,
11 subsidies, or other incentives to increase the
12 adoption of policies and controls or acquisition
13 of products and services that promote the cy-
14 bersecurity, for small organizations;

15 (D) as practicable, consult the certifi-
16 cations and requirement for cloud services de-
17 scribed in the final report of the Cyberspace So-
18 larium Commission established under section
19 1652 of the John S. McCain National Defense
20 Authorization Act for Fiscal Year 2019 (Public
21 Law 115–232; 132 Stat. 2140);

22 (E) describe evidence-based cybersecurity
23 controls and policies that improve cybersecurity
24 for small organizations; and

1 (F) with respect to the incentives described
2 in subparagraph (C), recommend measures that
3 can effectively improve cybersecurity at scale
4 for small organizations.

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

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

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

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

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

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

24 (B) the most significant cybersecurity
25 vulnerabilities facing small businesses;

1 (C) the most common challenges facing
2 small businesses in adopting the cybersecurity
3 guidance;

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

6 (E) the personnel small businesses dedicate
7 to cybersecurity (including the amount of total
8 personnel time, whether by employees or con-
9 tractors, dedicated to cybersecurity efforts).

10 (2) FORM.—The report required under para-
11 graph (1) shall be produced in unclassified form but
12 may contain a classified annex.

