

AMENDMENT TO RULES COMM. PRINT 117–13
OFFERED BY MR. TORRES OF NEW YORK

At the end of subtitle D of title XV, add the following new section:

1 **SEC. 15 ____ . STRATEGIC ASSESSMENT RELATING TO INNO-**
2 **VATION OF INFORMATION SYSTEMS AND CY-**
3 **BERSECURITY THREATS.**

4 (a) **RESPONSIBILITIES OF DIRECTOR.**—Section
5 2202(c)(3) of the Homeland Security Act of 2002 (6
6 U.S.C. 652) is amended by striking the semicolon at the
7 end and adding the following: “, including by carrying out
8 a periodic strategic assessment of the related programs
9 and activities of the Agency to ensure such programs and
10 activities contemplate the innovation of information sys-
11 tems and changes in cybersecurity risks and cybersecurity
12 threats;”

13 (b) **REPORT.**—

14 (1) **IN GENERAL.**—Not later than 120 days
15 after the date of the enactment of this Act and not
16 fewer than once every three years thereafter, the Di-
17 rector of the Cybersecurity and Infrastructure Secu-
18 rity Agency shall submit to the Committee on Home-
19 land Security of the House of Representatives and

1 the Committee on Homeland Security and Govern-
2 mental Affairs of the Senate a strategic assessment
3 for the purposes described in paragraph (2)

4 (2) PURPOSES.—The purposes described in this
5 paragraph are the following:

6 (A) A description of the existing programs
7 and activities administered in furtherance of
8 section 2202(c)(3) of the Homeland Security
9 Act of 2002 (6 U.S.C. 652).

10 (B) An assessment of the capability of ex-
11 isting programs and activities administered by
12 the Agency in furtherance of such section to
13 monitor for, manage, mitigate, and defend
14 against cybersecurity risks and cybersecurity
15 threats.

16 (C) An assessment of past or anticipated
17 technological trends or innovation of informa-
18 tion systems or information technology that
19 have the potential to affect the efficacy of the
20 programs and activities administered by the
21 Agency in furtherance of such section.

22 (D) A description of any changes in the
23 practices of the Federal workforce, such as in-
24 creased telework, affect the efficacy of the pro-

1 grams and activities administered by the Agen-
2 cy in furtherance of section 2202(c)(3).

3 (E) A plan to integrate innovative security
4 tools, technologies, protocols, activities, or pro-
5 grams to improve the programs and activities
6 administered by the Agency in furtherance of
7 such section.

8 (F) A description of any research and de-
9 velopment activities necessary to enhance the
10 programs and activities administered by the
11 Agency in furtherance of such section.

12 (G) A description of proposed changes to
13 existing programs and activities administered
14 by the Agency in furtherance of such section,
15 including corresponding milestones for imple-
16 mentation.

17 (H) Information relating to any new re-
18 sources or authorities necessary to improve the
19 programs and activities administered by the
20 Agency in furtherance of such section.

21 (c) DEFINITIONS.—In this section:

22 (1) The term “Agency” means the Cybersecu-
23 rity and Infrastructure Security Agency.

24 (2) The term “cybersecurity purpose” has the
25 meaning given such term in section 102(4) of the

1 Cybersecurity Information Sharing Act of 2015 (6
2 U.S.C. 1501(4)).

3 (3) The term “cybersecurity risk” has the
4 meaning given such term in section 2209(a)(2) of
5 the Homeland Security Act of 2002 (6 U.S.C.
6 659(a)(2)).

7 (4) The term “information system” has the
8 meaning given such term in section 3502(8) of title
9 44, United States Code.

10 (5) The term “information technology” has the
11 meaning given such term in 3502(9) of title 44,
12 United States Code.

13 (6) The term “telework” has the meaning given
14 the term in section 6501(3) of title 5, United States
15 Code.

