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:

SEC. 15. STRATEGIC ASSESSMENT RELATING TO INNOVATION OF INFORMATION SYSTEMS AND CYBERSECURITY THREATS.

(a) Responsibilities of Director.—Section 2202(c)(3) of the Homeland Security Act of 2002 (6 U.S.C. 652) is amended by striking the semicolon at the end and adding the following: “, including by carrying out a periodic strategic assessment of the related programs and activities of the Agency to ensure such programs and activities contemplate the innovation of information systems and changes in cybersecurity risks and cybersecurity threats;”

(b) Report.—

(1) In general.—Not later than 120 days after the date of the enactment of this Act and not fewer than once every three years thereafter, the Director of the Cybersecurity and Infrastructure Security Agency shall submit to the Committee on Homeland Security of the House of Representatives and...
the Committee on Homeland Security and Governmental Affairs of the Senate a strategic assessment for the purposes described in paragraph (2)

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


(B) An assessment of the capability of existing programs and activities administered by the Agency in furtherance of such section to monitor for, manage, mitigate, and defend against cybersecurity risks and cybersecurity threats.

(C) An assessment of past or anticipated technological trends or innovation of information systems or information technology that have the potential to affect the efficacy of the programs and activities administered by the Agency in furtherance of such section.

(D) A description of any changes in the practices of the Federal workforce, such as increased telework, affect the efficacy of the pro-
grams and activities administered by the Agency in furtherance of section 2202(c)(3).

(E) A plan to integrate innovative security tools, technologies, protocols, activities, or programs to improve the programs and activities administered by the Agency in furtherance of such section.

(F) A description of any research and development activities necessary to enhance the programs and activities administered by the Agency in furtherance of such section.

(G) A description of proposed changes to existing programs and activities administered by the Agency in furtherance of such section, including corresponding milestones for implementation.

(H) Information relating to any new resources or authorities necessary to improve the programs and activities administered by the Agency in furtherance of such section.

(c) DEFINITIONS.—In this section:

(1) The term “Agency” means the Cybersecurity and Infrastructure Security Agency.

(2) The term “cybersecurity purpose” has the meaning given such term in section 102(4) of the
Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501(4)).

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

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

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

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