AMENDMENT TO RULES COMM. PRINT 117–54
OFFERED BY MR. TORRES OF NEW YORK

Add at the end of title LII of division E the following:

SEC. 5206. BUILDING CYBER RESILIENCE AFTER SOLARWINDS.

(a) DEFINITIONS.—In this section:

(1) CRITICAL INFRASTRUCTURE.—The term “critical infrastructure” has the meaning given such term in section 1016(e) of Public Law 107–56 (42 U.S.C. 5195c(e)).

(2) DIRECTOR.—The term “Director” shall refer to the Director of the Cybersecurity and Infrastructure Security Agency.

(3) INFORMATION SYSTEM.—The term “information system” has the meaning given such term in section 2240 of the Homeland Security Act of 2002 (6 U.S.C. 681).

(4) SIGNIFICANT CYBER INCIDENT.—The term “significant cyber incident” has the meaning given such term in section 2240 of the Homeland Security Act of 2002.
(5) **SolarWinds Incident.**—The term “SolarWinds incident” refers to the significant cyber incident that prompted the establishment of a Unified Cyber Coordination Group, as provided by section V(B)(2) of Presidential Policy Directive 41, in December 2020.

(b) **SolarWinds Investigation and Report.**—

(1) **Investigation.**—The Director, in consultation with the National Cyber Director and the heads of other relevant Federal departments and agencies, shall carry out an investigation to evaluate the impact of the SolarWinds incident on information systems owned and operated by Federal departments and agencies, and, to the extent practicable, other critical infrastructure.

(2) **Elements.**—In carrying out subsection (b), the Director shall review the following:

(A) The extent to which Federal information systems were accessed, compromised, or otherwise impacted by the SolarWinds incident, and any potential ongoing security concerns or consequences arising from such incident.

(B) The extent to which information systems that support other critical infrastructure were accessed, compromised, or otherwise im-
Racted by the SolarWinds incident, where such
information is available to the Director.

(C) Any ongoing security concerns or con-
sequences arising from the SolarWinds incident,
including any sensitive information that may
have been accessed or exploited in a manner
that poses a threat to national security.

(D) Implementation of Executive Order
14028 (Improving the Nation’s Cybersecurity
(May 12, 2021)).

(E) Efforts taken by the Director, the
heads of Federal departments and agencies,
and critical infrastructure owners and operators
to address cybersecurity vulnerabilities and
mitigate risks associated with the SolarWinds
incident.

(c) REPORT.—Not later than 120 days after the date
of the enactment of this Act, the Director shall submit
to the Committee on Homeland Security in the House of
Representatives and Committee on Homeland Security
and Government Affairs in the Senate a report that in-
cludes the following:

(1) Findings for each of the elements specified
in subsection (b).
(2) Recommendations to address security gaps, improve incident response efforts, and prevent similar cyber incidents.

(3) Any areas where the Director lacked the information necessary to fully review and assessment such elements, the reason the information necessary was unavailable, and recommendations to close such informational gaps.

(d) GAO Report on Cyber Safety Review Board.—Not later than one year after the date of the enactment of this Act, the Comptroller General of the United States shall evaluate the activities of the Cyber Safety Review Board established pursuant to Executive Order 14028 (Improving the Nation’s Cybersecurity (May 12, 2021)), with a focus on the Board’s inaugural review announced in February 2022, and assess whether the Board has the authorities, resources, and expertise necessary to carry out its mission of reviewing and assessing significant cyber incidents.