

**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:

1 **SEC. 5206. BUILDING CYBER RESILIENCE AFTER**  
2 **SOLARWINDS.**

3 (a) DEFINITIONS.—In this section:

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

8 (2) DIRECTOR.—The term “Director” shall  
9 refer to the Director of the Cybersecurity and Infra-  
10 structure Security Agency.

11 (3) INFORMATION SYSTEM.—The term “infor-  
12 mation system” has the meaning given such term in  
13 section 2240 of the Homeland Security Act of 2002  
14 (6 U.S.C. 681).

15 (4) SIGNIFICANT CYBER INCIDENT.—The term  
16 “significant cyber incident” has the meaning given  
17 such term in section 2240 of the Homeland Security  
18 Act of 2002.

1           (5) SOLARWINDS INCIDENT.—The term  
2           “SolarWinds incident” refers to the significant cyber  
3           incident that prompted the establishment of a Uni-  
4           fied Cyber Coordination Group, as provided by sec-  
5           tion V(B)(2) of Presidential Policy Directive 41, in  
6           December 2020.

7           (b) SOLARWINDS INVESTIGATION AND REPORT.—

8           (1) INVESTIGATION.—The Director, in con-  
9           sultation with the National Cyber Director and the  
10          heads of other relevant Federal departments and  
11          agencies, shall carry out an investigation to evaluate  
12          the impact of the SolarWinds incident on informa-  
13          tion systems owned and operated by Federal depart-  
14          ments and agencies, and, to the extent practicable,  
15          other critical infrastructure.

16          (2) ELEMENTS.—In carrying out subsection  
17          (b), the Director shall review the following:

18                 (A) The extent to which Federal informa-  
19                 tion systems were accessed, compromised, or  
20                 otherwise impacted by the SolarWinds incident,  
21                 and any potential ongoing security concerns or  
22                 consequences arising from such incident.

23                 (B) The extent to which information sys-  
24                 tems that support other critical infrastructure  
25                 were accessed, compromised, or otherwise im-

1           pacted by the SolarWinds incident, where such  
2           information is available to the Director.

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

8           (D) Implementation of Executive Order  
9           14028 (Improving the Nation's Cybersecurity  
10          (May 12, 2021)).

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

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

23                 (1) Findings for each of the elements specified  
24                 in subsection (b).

1           (2) Recommendations to address security gaps,  
2           improve incident response efforts, and prevent simi-  
3           lar cyber incidents.

4           (3) Any areas where the Director lacked the in-  
5           formation necessary to fully review and assessment  
6           such elements, the reason the information necessary  
7           was unavailable, and recommendations to close such  
8           informational gaps.

9           (d) GAO REPORT ON CYBER SAFETY REVIEW  
10          BOARD.—Not later than one year after the date of the  
11          enactment of this Act, the Comptroller General of the  
12          United States shall evaluate the activities of the Cyber  
13          Safety Review Board established pursuant to Executive  
14          Order 14028 (Improving the Nation’s Cybersecurity (May  
15          12, 2021)), with a focus on the Board’s inaugural review  
16          announced in February 2022, and assess whether the  
17          Board has the authorities, resources, and expertise nec-  
18          essary to carry out its mission of reviewing and assessing  
19          significant cyber incidents.

