

117TH CONGRESS
2D SESSION

H. R. 8279

To require the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security to submit a report on the impact of the SolarWinds cyber incident on information systems owned and operated by Federal departments and agencies and other critical infrastructure, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JULY 1, 2022

Mr. TORRES of New York introduced the following bill; which was referred to the Committee on Oversight and Reform, and in addition to the Committee on Homeland Security, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To require the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security to submit a report on the impact of the SolarWinds cyber incident on information systems owned and operated by Federal departments and agencies and other critical infrastructure, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

1 **SECTION 1. SHORT TITLE.**

2 This Act may be cited as the “Building Cyber Resil-
3 ience After SolarWinds Act of 2022”.

4 **SEC. 2. BUILDING CYBER RESILIENCE AFTER SOLARWINDS.**

5 (a) DEFINITIONS.—In this section:

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

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

13 (3) INFORMATION SYSTEM.—The term “infor-
14 mation system” has the meaning given such term in
15 section 2240 of the Homeland Security Act of 2002
16 (6 U.S.C. 681).

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

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

1 (b) SOLARWINDS INVESTIGATION AND REPORT.—

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

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

12 (A) The extent to which Federal informa-
13 tion systems were accessed, compromised, or
14 otherwise impacted by the SolarWinds incident,
15 and any potential ongoing security concerns or
16 consequences arising from such incident.

17 (B) The extent to which information sys-
18 tems that support other critical infrastructure
19 were accessed, compromised, or otherwise im-
20 pacted by the SolarWinds incident, where such
21 information is available to the Director.

22 (C) Any ongoing security concerns or con-
23 sequences arising from the SolarWinds incident,
24 including any sensitive information that may

1 have been accessed or exploited in a manner
2 that poses a threat to national security.

3 (D) Implementation of Executive Order
4 14028 (Improving the Nation's Cybersecurity
5 (May 12, 2021)).

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

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

18 (1) Findings for each of the elements specified
19 in subsection (b).

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

23 (3) Any areas where the Director lacked the in-
24 formation necessary to fully review and assessment
25 such elements, the reason the information necessary

1 was unavailable, and recommendations to close such
2 informational gaps.

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

○