I

118TH CONGRESS
1ST SESSION

H. R. 3166

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

MAY 9, 2023

Mr. TORRES of New York introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Oversight and Accountability, 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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Building Cyber Resilience After SolarWinds Act of 2023''.

SEC. 2. 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'' means the Director of the Cybersecurity and Infrastructure Security Agency.

(3) INFORMATION SYSTEM.—The term ''information system'' has the meaning given such term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(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 (6 U.S.C. 681).

(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 impacted by the SolarWinds incident, where such information is available to the Director.

(C) Any ongoing security concerns or consequences 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 of the House of Representatives and Committee on Homeland Security and Governmental Affairs of the Senate a report that includes 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 with respect to which the Director lacked the information necessary to fully review and assessment such elements, the reason the infor-

mation 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.

○