Calendar No. 62

116TH CONGRESS
1ST SESSION

S. 315

[Report No. 116–27]

To authorize cyber hunt and incident response teams at the Department of Homeland Security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JANUARY 31, 2019

Ms. HASSAN (for herself, Mr. PORTMAN, and Mr. PETERS) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

APRIL 8, 2019

Reported by Mr. JOHNSON, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

A BILL

To authorize cyber hunt and incident response teams at the Department of Homeland Security, 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 "DHS Cyber Hunt and Incident Response Teams Act of 2019".~~

SEC. 2. DEPARTMENT OF HOMELAND SECURITY CYBER HUNT AND INCIDENT RESPONSE TEAMS.

(a) IN GENERAL.—Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (d)(1)(B)(iv), by inserting ", including cybersecurity specialists" after "entities";

(2) by redesignating subsections (f) through (m) as subsections (g) through (n), respectively;

(3) by inserting after subsection (e) the following:

"(f) CYBER HUNT AND INCIDENT RESPONSE TEAMS.—

"(1) IN GENERAL.—The Center shall maintain cyber hunt and incident response teams for the purpose of leading Federal asset response activities and providing timely technical assistance to Federal and non-Federal entities, including across all critical infrastructure sectors, regarding actual or potential security incidents, as appropriate and upon request, including—

"(A) assistance to asset owners and operators in restoring services following a cyber incident;

"(B) identification and analysis of cybersecurity risk and unauthorized cyber activity;

"(C) mitigation strategies to prevent, deter, and protect against cybersecurity risks;

"(D) recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as appropriate; and

"(E) such other capabilities as the Secretary determines appropriate.

"(2) ASSOCIATED METRICS.—The Center shall continually assess and evaluate the cyber hunt and incident response teams and the operations of those cyber hunt and incident response teams using robust metrics.

"(3) REPORT.—At the conclusion of each of the first 4 fiscal years after the date of enactment of the DHS Cyber Hunt and Incident Response Teams Act of 2019, the Center shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that includes—

"(A) information relating to the metrics used for evaluation and assessment of the cyber hunt and incident response teams and oper-

ations under paragraph (2), including the resources and staffing of those cyber hunt and incident response teams; and

"(B) for the period covered by the report—

"(i) the total number of incident response requests received;

"(ii) the number of incident response tickets opened; and

"(iii) a statement of—

"(I) all interagency staffing of cyber hunt and incident response teams; and

"(II) the interagency collaborations established to support cyber hunt and incident response teams.

"(4) CYBERSECURITY SPECIALISTS.—After notice to, and with the approval of, the entity requesting action by or technical assistance from the Center, the Secretary may include cybersecurity specialists from the private sector on a cyber hunt and incident response team."; and

(4) in subsection (g), as so redesignated—

~~(A) in paragraph (1), by inserting ", or any team or activity of the Center," after "Center"; and~~

~~(B) in paragraph (2), by inserting ", or any team or activity of the Center," after "Center".~~

~~(b) NO ADDITIONAL FUNDS AUTHORIZED.—No additional funds are authorized to be appropriated to carry out the requirements of this Act and the amendments made by this Act. Such requirements shall be carried out using amounts otherwise authorized to be appropriated.~~

SECTION 1. SHORT TITLE.

This Act may be cited as the "DHS Cyber Hunt and Incident Response Teams Act of 2019".

SEC. 2. DEPARTMENT OF HOMELAND SECURITY CYBER HUNT AND INCIDENT RESPONSE TEAMS.

(a) IN GENERAL.—Section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659) is amended—

(1) in subsection (d)(1)(B)(iv), by inserting ", including cybersecurity specialists" after "entities";

(2) by redesignating subsections (f) through (m) as subsections (g) through (n), respectively;

(3) by inserting after subsection (e) the following:

"(f) CYBER HUNT AND INCIDENT RESPONSE TEAMS.—

"(1) IN GENERAL.—The Center shall maintain cyber hunt and incident response teams for the purpose of leading Federal asset response activities and providing timely technical assistance to Federal and non-Federal entities, including across all critical infrastructure sectors, regarding actual or potential security incidents, as appropriate and upon request, including—

"(A) assistance to asset owners and operators in restoring services following a cyber incident;

"(B) identification and analysis of cybersecurity risk and unauthorized cyber activity;

"(C) mitigation strategies to prevent, deter, and protect against cybersecurity risks;

"(D) recommendations to asset owners and operators for improving overall network and control systems security to lower cybersecurity risks, and other recommendations, as appropriate; and

"(E) such other capabilities as the Secretary determines appropriate.

"(2) ASSOCIATED METRICS.—The Center shall—

"(A) define the goals and desired outcomes for each cyber hunt and incident response team; and

"(B) develop metrics—

"(i) to measure the effectiveness and efficiency of each cyber hunt and incident response team in achieving the goals and desired outcomes defined under subparagraph (A); and

"(ii) that—

"(I) are quantifiable and actionable; and

"(II) the Center shall use to improve the effectiveness and accountability of, and service delivery by, cyber hunt and incident response teams.

"(3) CYBERSECURITY SPECIALISTS.—After notice to, and with the approval of, the entity requesting action by or technical assistance from the Center, the Secretary may include cybersecurity specialists from the private sector on a cyber hunt and incident response team."; and

(4) in subsection (g), as so redesignated—

(A) in paragraph (1), by inserting ", or any team or activity of the Center," after "Center"; and

(B) in paragraph (2), by inserting ", or any team or activity of the Center," after "Center".

(b) REPORT.—

(1) DEFINITIONS.—In this subsection—

(A) the term "Center" means the national cybersecurity and communications integration center established under section 2209(b) of the Homeland Security Act of 2002 (6 U.S.C. 659(b));

(B) the term "cyber hunt and incident response team" means a cyber hunt and incident response team maintained under section 2209(f) of the Homeland Security Act of 2002 (6 U.S.C. 659(f)), as added by this Act; and

(C) the term "incident" has the meaning given the term in section 2209(a) of the Homeland Security Act of 2002 (6 U.S.C. 659(a)).

(2) REPORT.—At the conclusion of each of the first 4 fiscal years after the date of enactment of the DHS Cyber Hunt and Incident Response Teams Act of 2019, the Center shall submit to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives a report that includes—

(A) information relating to the metrics used for evaluation and assessment of the cyber hunt and incident response teams and operations under section 2209(f)(2) of the Homeland Security Act of 2002 (6 U.S.C. 659(f)(2)), as added by this Act, including the resources and staffing of those cyber hunt and incident response teams; and

(B) for the period covered by the report—

(i) the total number of incident response requests received;

(ii) the number of incident response tickets opened; and

(iii) a statement of—

(I) all interagency staffing of cyber hunt and incident response teams; and

(II) the interagency collaborations established to support cyber hunt and incident response teams.

(c) NO ADDITIONAL FUNDS AUTHORIZED.—No additional funds are authorized to be appropriated to carry out the requirements of this Act and the amendments made by this Act. Such requirements shall be carried out using amounts otherwise authorized to be appropriated.

Calendar No. 62

116TH CONGRESS
1ST SESSION

S. 315

[Report No. 116–27]

A BILL

To authorize cyber hunt and incident response teams at the Department of Homeland Security, and for other purposes.

APRIL 8, 2019

Reported with an amendment