

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.

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

3 **SECTION 1. SHORT TITLE.**

4 ~~This Act may be cited as the “DHS Cyber Hunt and~~
5 ~~Incident Response Teams Act of 2019”.~~

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

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

5 (1) in subsection (d)(1)(B)(iv), by inserting “,
 6 including cybersecurity specialists” after “entities”;

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

9 (3) by inserting after subsection (e) the fol-
 10 lowing:

11 “(f) **CYBER HUNT AND INCIDENT RESPONSE**
 12 **TEAMS.**—

13 “(1) **IN GENERAL.**—The Center shall maintain
 14 cyber hunt and incident response teams for the pur-
 15 pose of leading Federal asset response activities and
 16 providing timely technical assistance to Federal and
 17 non-Federal entities, including across all critical in-
 18 frastructure sectors, regarding actual or potential
 19 security incidents, as appropriate and upon request,
 20 including—

21 “(A) assistance to asset owners and opera-
 22 tors in restoring services following a cyber inci-
 23 dent;

24 “(B) identification and analysis of cyberse-
 25 curity risk and unauthorized cyber activity;

1 “(C) mitigation strategies to prevent,
2 deter, and protect against cybersecurity risks;

3 “(D) recommendations to asset owners and
4 operators for improving overall network and
5 control systems security to lower cybersecurity
6 risks; and other recommendations; as appro-
7 priate; and

8 “(E) such other capabilities as the Sec-
9 retary determines appropriate.

10 “(2) ASSOCIATED METRICS.—The Center shall
11 continually assess and evaluate the cyber hunt and
12 incident response teams and the operations of those
13 cyber hunt and incident response teams using robust
14 metrics.

15 “(3) REPORT.—At the conclusion of each of the
16 first 4 fiscal years after the date of enactment of the
17 DHS Cyber Hunt and Incident Response Teams Act
18 of 2019, the Center shall submit to the Committee
19 on Homeland Security and Governmental Affairs of
20 the Senate and the Committee on Homeland Secu-
21 rity of the House of Representatives a report that
22 includes—

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

1 ations under paragraph (2), including the re-
 2 sources and staffing of those cyber hunt and in-
 3 cident response teams; and

4 “~~(B)~~ for the period covered by the re-
 5 port—

6 “~~(i)~~ the total number of incident re-
 7 sponse requests received;

8 “~~(ii)~~ the number of incident response
 9 tickets opened; and

10 “~~(iii)~~ a statement of—

11 “~~(I)~~ all interagency staffing of
 12 cyber hunt and incident response
 13 teams; and

14 “~~(II)~~ the interagency collabora-
 15 tions established to support cyber
 16 hunt and incident response teams.

17 “~~(4)~~ CYBERSECURITY SPECIALISTS.—After no-
 18 tice to, and with the approval of, the entity request-
 19 ing action by or technical assistance from the Cen-
 20 ter, the Secretary may include cybersecurity special-
 21 ists from the private sector on a cyber hunt and in-
 22 cident response team.”; and

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

1 “(1) *IN GENERAL.*—*The Center shall maintain*
2 *cyber hunt and incident response teams for the pur-*
3 *pose of leading Federal asset response activities and*
4 *providing timely technical assistance to Federal and*
5 *non-Federal entities, including across all critical in-*
6 *frastructure sectors, regarding actual or potential se-*
7 *curity incidents, as appropriate and upon request, in-*
8 *cluding—*

9 “(A) *assistance to asset owners and opera-*
10 *tors in restoring services following a cyber inci-*
11 *dent;*

12 “(B) *identification and analysis of cyberse-*
13 *curity risk and unauthorized cyber activity;*

14 “(C) *mitigation strategies to prevent, deter,*
15 *and protect against cybersecurity risks;*

16 “(D) *recommendations to asset owners and*
17 *operators for improving overall network and con-*
18 *trol systems security to lower cybersecurity risks,*
19 *and other recommendations, as appropriate; and*

20 “(E) *such other capabilities as the Sec-*
21 *retary determines appropriate.*

22 “(2) *ASSOCIATED METRICS.*—*The Center shall—*

23 “(A) *define the goals and desired outcomes*
24 *for each cyber hunt and incident response team;*
25 *and*

1 “(B) develop metrics—

2 “(i) to measure the effectiveness and ef-
3 ficiency of each cyber hunt and incident re-
4 sponse team in achieving the goals and de-
5 sired outcomes defined under subparagraph
6 (A); and

7 “(ii) that—

8 “(I) are quantifiable and action-
9 able; and

10 “(II) the Center shall use to im-
11 prove the effectiveness and account-
12 ability of, and service delivery by,
13 cyber hunt and incident response
14 teams.

15 “(3) CYBERSECURITY SPECIALISTS.—After notice
16 to, and with the approval of, the entity requesting ac-
17 tion by or technical assistance from the Center, the
18 Secretary may include cybersecurity specialists from
19 the private sector on a cyber hunt and incident re-
20 sponse team.”; and

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

22 (A) in paragraph (1), by inserting “, or
23 any team or activity of the Center,” after “Cen-
24 ter”; and

1 (B) in paragraph (2), by inserting “, or
2 any team or activity of the Center,” after “Cen-
3 ter”.

4 (b) *REPORT.*—

5 (1) *DEFINITIONS.*—*In this subsection—*

6 (A) the term “Center” means the national
7 cybersecurity and communications integration
8 center established under section 2209(b) of the
9 Homeland Security Act of 2002 (6 U.S.C.
10 659(b));

11 (B) the term “cyber hunt and incident re-
12 sponse team” means a cyber hunt and incident
13 response team maintained under section 2209(f)
14 of the Homeland Security Act of 2002 (6 U.S.C.
15 659(f)), as added by this Act; and

16 (C) the term “incident” has the meaning
17 given the term in section 2209(a) of the Home-
18 land Security Act of 2002 (6 U.S.C. 659(a)).

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

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

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

10 (i) the total number of incident re-
11 sponse requests received;

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

14 (iii) a statement of—

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

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

21 (c) *NO ADDITIONAL FUNDS AUTHORIZED.*—No addi-
22 tional funds are authorized to be appropriated to carry out
23 the requirements of this Act and the amendments made by
24 this Act. Such requirements shall be carried out using
25 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