

Calendar No. 458

116TH CONGRESS
2D SESSION**S. 3207****[Report No. 116–227]**

To require the Director of the Cybersecurity and Infrastructure Security Agency to establish a Cybersecurity State Coordinator in each State, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JANUARY 16, 2020

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

JUNE 1, 2020

Reported by Mr. JOHNSON, with an amendment

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

To require the Director of the Cybersecurity and Infrastructure Security Agency to establish a Cybersecurity State Coordinator in each State, 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 “Cybersecurity State
3 Coordinator Act of 2020”.

4 **SEC. 2. FINDINGS.**

5 Congress finds that—

6 (1) cyber threats, such as ransomware, against
7 State, local, Tribal, and territorial entities have
8 grown at an alarming rate;

9 (2) State, local, Tribal, and territorial entities
10 face a growing threat from advanced persistent
11 threat actors, hostile nation states, criminal groups,
12 and other malicious cyber actors;

13 (3) there is an urgent need for greater engage-
14 ment and expertise from the Federal Government to
15 help these entities build their resilience and defenses;
16 and

17 (4) coordination within Federal entities and be-
18 tween Federal and non-Federal entities, including
19 State, local, Tribal, and territorial governments, In-
20 formation Sharing and Analysis Centers, election of-
21 ficials, State adjutants general, and other non-Fed-
22 eral entities, is critical to anticipating, preventing,
23 managing, and recovering from cyberattacks.

1 **SEC. 3. CYBERSECURITY STATE COORDINATOR.**

2 (a) IN GENERAL.—Subtitle A of title XXII of the
3 Homeland Security Act of 2002 (6 U.S.C. 651 et seq.)
4 is amended—

5 (1) in section 2202(c) (6 U.S.C. 652(c))—

6 (A) in paragraph (10), by striking “and”
7 at the end;

8 (B) by redesignating paragraph (11) as
9 paragraph (12); and

10 (C) by inserting after paragraph (10) the
11 following:

12 “(11) appoint a Cybersecurity State Coordi-
13 nator in each State, as described in section 2215;
14 and”; and

15 (2) by adding at the end the following:

16 **“SEC. 2215. CYBERSECURITY STATE COORDINATOR.**

17 “(a) APPOINTMENT.—The Director shall appoint an
18 employee of the Agency in each State who shall serve as
19 the Cybersecurity State Coordinator.

20 “(b) DUTIES.—The duties of a Cybersecurity State
21 Coordinator appointed under subsection (b) shall in-
22 clude—

23 “(1) building strategic relationships across Fed-
24 eral and non-Federal entities by advising on estab-
25 lishing governance structures to facilitate developing
26 and maintaining secure and resilient infrastructure;

1 “(2) serving as a principal Federal cybersecu-
2 rity risk advisor and coordinating between Federal
3 and non-Federal entities to support preparation, re-
4 sponse, and remediation efforts relating to cyberse-
5 curity risks and incidents;

6 “(3) facilitating the sharing of cyber threat in-
7 formation between Federal and non-Federal entities
8 to improve understanding of cybersecurity risks and
9 situational awareness of cybersecurity incidents;

10 “(4) raising awareness of the financial, tech-
11 nical, and operational resources available from the
12 Federal Government to non-Federal entities to in-
13 crease resilience against cyber threats;

14 “(5) supporting training, exercises, and plan-
15 ning for continuity of operations to expedite recovery
16 from cybersecurity incidents, including ransomware;

17 “(6) serving as a principal point of contact for
18 non-Federal entities to engage with the Federal Gov-
19 ernment on preparing, managing, and responding to
20 cybersecurity incidents;

21 “(7) assisting non-Federal entities in developing
22 and coordinating vulnerability disclosure programs
23 consistent with Federal and information security in-
24 dustry standards; and

1 “(8) performing such other duties as necessary
 2 to achieve the goal of managing cybersecurity risks
 3 in the United States and reducing the impact of
 4 cyber threats to non-Federal entities.

5 “(e) FEEDBACK.—The Director shall take into ac-
 6 count relevant feedback provided by State and local offi-
 7 cials regarding the appointment, and State and local offi-
 8 cials and other non-Federal entities regarding the per-
 9 formance, of the Cybersecurity State Coordinator of a
 10 State.”.

11 (b) OVERSIGHT.—Not later than 1 year after the
 12 date of enactment of this Act, the Director of the Cyberse-
 13 curity and Infrastructure Security Agency shall provide to
 14 the Committee on Homeland Security and Governmental
 15 Affairs of the Senate and the Committee on Homeland
 16 Security of the House of Representatives a briefing on the
 17 placement and efficacy of the Cybersecurity State Coordi-
 18 nators appointed under section 2215 of the Homeland Se-
 19 curity Act of 2002, as added by subsection (a).

20 (c) RULE OF CONSTRUCTION.—Nothing in this sec-
 21 tion or the amendments made by this section shall be con-
 22 strued to affect or otherwise modify the authority of Fed-
 23 eral law enforcement agencies with respect to investiga-
 24 tions relating to cybersecurity incidents.

1 ~~(d) TECHNICAL AND CONFORMING AMENDMENT.—~~

2 The table of contents in section 1(b) of the Homeland Se-
 3 curity Act of 2002 (Public Law 107–296; 116 Stat. 2135)
 4 is amended by inserting after the item relating to section
 5 2214 the following:

 “Sec. 2215. Cybersecurity State Coordinator.”.

6 **SECTION 1. SHORT TITLE.**

7 *This Act may be cited as the “Cybersecurity State Co-*
 8 *ordinator Act of 2020”.*

9 **SEC. 2. FINDINGS.**

10 *Congress finds that—*

11 *(1) cyber threats, such as ransomware, against*
 12 *State, local, Tribal, and territorial entities have*
 13 *grown at an alarming rate;*

14 *(2) State, local, Tribal, and territorial entities*
 15 *face a growing threat from advanced persistent threat*
 16 *actors, hostile nation states, criminal groups, and*
 17 *other malicious cyber actors;*

18 *(3) there is an urgent need for greater engage-*
 19 *ment and expertise from the Federal Government to*
 20 *help these entities build their resilience and defenses;*
 21 *and*

22 *(4) coordination within Federal entities and be-*
 23 *tween Federal and non-Federal entities, including*
 24 *State, local, Tribal, and territorial governments, In-*
 25 *formation Sharing and Analysis Centers, election offi-*

1 *cials, State adjutants general, and other non-Federal*
 2 *entities, is critical to anticipating, preventing, man-*
 3 *aging, and recovering from cyberattacks.*

4 **SEC. 3. CYBERSECURITY STATE COORDINATOR.**

5 *(a) IN GENERAL.—Subtitle A of title XXII of the*
 6 *Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is*
 7 *amended—*

8 *(1) in section 2202(c) (6 U.S.C. 652(c))—*

9 *(A) in paragraph (10), by striking “and”*
 10 *at the end;*

11 *(B) by redesignating paragraph (11) as*
 12 *paragraph (12); and*

13 *(C) by inserting after paragraph (10) the*
 14 *following:*

15 *“(11) appoint a Cybersecurity State Coordinator*
 16 *in each State, as described in section 2215; and”;* and

17 *(2) by adding at the end the following:*

18 **“SEC. 2215. CYBERSECURITY STATE COORDINATOR.**

19 *“(a) APPOINTMENT.—The Director shall appoint an*
 20 *employee of the Agency in each State, with the appropriate*
 21 *cybersecurity qualifications and expertise, who shall serve*
 22 *as the Cybersecurity State Coordinator.*

23 *“(b) DUTIES.—The duties of a Cybersecurity State Co-*
 24 *ordinator appointed under subsection (a) shall include—*

1 “(1) *building strategic relationships across Fed-*
2 *eral and, on a voluntary basis, non-Federal entities*
3 *by advising on establishing governance structures to*
4 *facilitate the development and maintenance of secure*
5 *and resilient infrastructure;*

6 “(2) *serving as a Federal cybersecurity risk ad-*
7 *visor and coordinating between Federal and, on a vol-*
8 *untary basis, non-Federal entities to support prepa-*
9 *ration, response, and remediation efforts relating to*
10 *cybersecurity risks and incidents;*

11 “(3) *facilitating the sharing of cyber threat in-*
12 *formation between Federal and, on a voluntary basis,*
13 *non-Federal entities to improve understanding of cy-*
14 *bersecurity risks and situational awareness of cyberse-*
15 *curity incidents;*

16 “(4) *raising awareness of the financial, tech-*
17 *nical, and operational resources available from the*
18 *Federal Government to non-Federal entities to in-*
19 *crease resilience against cyber threats;*

20 “(5) *supporting training, exercises, and plan-*
21 *ning for continuity of operations to expedite recovery*
22 *from cybersecurity incidents, including ransomware;*

23 “(6) *serving as a principal point of contact for*
24 *non-Federal entities to engage, on a voluntary basis,*

1 *with the Federal Government on preparing, man-*
2 *aging, and responding to cybersecurity incidents;*

3 “(7) *assisting non-Federal entities in developing*
4 *and coordinating vulnerability disclosure programs*
5 *consistent with Federal and information security in-*
6 *dustry standards; and*

7 “(8) *performing such other duties as determined*
8 *necessary by the Director to achieve the goal of man-*
9 *aging cybersecurity risks in the United States and re-*
10 *ducing the impact of cyber threats to non-Federal en-*
11 *tities.*

12 “(c) *FEEDBACK.—The Director shall consult with rel-*
13 *evant State and local officials regarding the appointment,*
14 *and State and local officials and other non-Federal entities*
15 *regarding the performance, of the Cybersecurity State Coor-*
16 *dinator of a State.”.*

17 “(b) *OVERSIGHT.—The Director of the Cybersecurity*
18 *and Infrastructure Security Agency shall provide to the*
19 *Committee on Homeland Security and Governmental Af-*
20 *airs of the Senate and the Committee on Homeland Secu-*
21 *rity of the House of Representatives a briefing on the place-*
22 *ment and efficacy of the Cybersecurity State Coordinators*
23 *appointed under section 2215 of the Homeland Security Act*
24 *of 2002, as added by subsection (a)—*

1 (1) *not later than 1 year after the date of enact-*
2 *ment of this Act; and*

3 (2) *not later than 2 years after providing the*
4 *first briefing under this subsection.*

5 (c) *RULE OF CONSTRUCTION.—Nothing in this section*
6 *or the amendments made by this section shall be construed*
7 *to affect or otherwise modify the authority of Federal law*
8 *enforcement agencies with respect to investigations relating*
9 *to cybersecurity incidents.*

10 (d) *TECHNICAL AND CONFORMING AMENDMENT.—The*
11 *table of contents in section 1(b) of the Homeland Security*
12 *Act of 2002 (Public Law 107–296; 116 Stat. 2135) is*
13 *amended by inserting after the item relating to section 2214*
14 *the following:*

 “Sec. 2215. *Cybersecurity State Coordinator.*”.

Calendar No. 458

116TH CONGRESS
2^D Session

S. 3207

[Report No. 116–227]

A BILL

To require the Director of the Cybersecurity and Infrastructure Security Agency to establish a Cybersecurity State Coordinator in each State, and for other purposes.

JUNE 1, 2020

Reported with an amendment