

.....
(Original Signature of Member)

118TH CONGRESS
2D SESSION

H. R. _____

To amend the Homeland Security Act of 2002 to establish within the Cybersecurity and Infrastructure Security Agency a Joint Cyber Defense Collaborative, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

Mr. SWALWELL introduced the following bill; which was referred to the
Committee on Homeland Security

A BILL

To amend the Homeland Security Act of 2002 to establish within the Cybersecurity and Infrastructure Security Agency a Joint Cyber Defense Collaborative, 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 “Joint Cyber Defense
5 Collaborative Act”.

1 **SEC. 2. ESTABLISHMENT OF JOINT CYBER DEFENSE COL-**
2 **LABORATIVE.**

3 (a) IN GENERAL.—Section 2216 of the Homeland
4 Security Act of 2002 (6 U.S.C. 665b) is amended—

5 (1) in the section heading, by striking “**JOINT**
6 **CYBER PLANNING OFFICE**” and inserting “**JOINT**
7 **CYBER DEFENSE COLLABORATIVE**”;

8 (2) by striking subsection (a);

9 (3) by redesignating subsections (b) through (f)
10 as subsections (f) through (j), respectively;

11 (4) by inserting before subsection (f), as so re-
12 designated, the following new subsections:

13 “(a) IN GENERAL.—The Agency shall maintain the
14 ‘Joint Cyber Defense Collaborative’ program (in this sec-
15 tion referred to as the ‘Collaborative’) to support enhanced
16 public-private partnerships across critical infrastructure
17 sectors for collective cyber defense operations, information
18 sharing, and operational collaboration, and develop, for
19 Federal and non-Federal entities, plans for cyber defense
20 operations, including the development of a set of coordi-
21 nated actions to detect, prevent, limit, prepare for, miti-
22 gate, protect against, respond to, recover from, and build
23 resilience to cybersecurity risks, security vulnerabilities,
24 and incidents, and cybersecurity threats to, and incidents
25 or active malicious cyber operations targeting, critical in-
26 frastructure or national interests. The Collaborative shall

1 be headed by a senior official of the Agency selected by
2 the Director.

3 “(b) FUNCTIONS.—The Collaborative shall carry out
4 the following:

5 “(1) Maintain strategic, operational partner-
6 ships with entities and organizations with diverse cy-
7 bersecurity roles, expertise, and situational aware-
8 ness that will enhance the Agency’s situational
9 awareness of cybersecurity risks, cybersecurity
10 threats, and active malicious cyber operations, in-
11 cluding with cybersecurity and technology compa-
12 nies, critical infrastructure owners and operators, se-
13 curity researchers and academic institutions, non-
14 governmental organizations, information system ven-
15 dors, manufacturers, and foreign government enti-
16 ties in accordance with subsection (c), and other en-
17 tities as appropriate.

18 “(2) Develop, for public and private sector enti-
19 ties, plans for cyber defense operations, including
20 the development of a set of coordinated actions to
21 support governmental and non-governmental entities
22 to—

23 “(A) protect, detect, respond to, and re-
24 cover from cybersecurity risks, cybersecurity

1 threats, active malicious cyber operations, or in-
2 cidents; or

3 “(B) limit, mitigate, or defend against ac-
4 tive or anticipated malicious cyber operations
5 that pose a potential risk to critical infrastruc-
6 ture or national security interests.

7 “(3) Develop plans for governmental and non-
8 governmental entities, including cyber incident re-
9 sponse plans under 2210(c), plans relating to threat-
10 focused campaigns, and plans to address long-term
11 cybersecurity priorities.

12 “(4) Gather, analyze, synthesize, and rapidly
13 share information relating to cybersecurity threats
14 and warnings to inform collective cyber defense oper-
15 ations, either through direct engagement or through
16 the sharing of cybersecurity guidance through indus-
17 try organizations to drive action across all stake-
18 holder communities.

19 “(5) Facilitate the development and publication
20 of joint analyses with Government and non-govern-
21 ment partners, as well as international partners, as
22 appropriate, regarding threat actors, cybersecurity
23 risks, cybersecurity threats, active malicious cyber
24 operations, and incidents within and across critical
25 infrastructure sectors, to enhance awareness of ad-

1 versary tactics, techniques, and procedures and pro-
2 vide recommendations for mitigation.

3 “(6) Utilizing mechanisms that enable confiden-
4 tial real-time information sharing and dissemination
5 of technical products between the Collaborative and
6 its partners.

7 “(7) Develop processes and procedures to rap-
8 idly share with non-governmental entities timely and
9 actionable cyber threat intelligence and information
10 from Government entities, including the
11 Collaborative’s partners, for purposes of informing
12 joint activities within the Collaborative, as well as
13 proactive defense actions to defend critical infra-
14 structure and non-Federal networks.

15 “(8) Establish, as appropriate, focused initia-
16 tives designed to respond to significant, emergent, or
17 evolving cybersecurity risks or cybersecurity threats
18 to, or active malicious cyber operations targeting,
19 critical infrastructure sectors or technologies, includ-
20 ing industrial control systems.

21 “(9) Develop plans for cyber defense operations
22 for Federal Government and non-Federal Govern-
23 ment entities, as well as plans to respond to specific
24 cybersecurity risks, cybersecurity threats, active ma-
25 licious cyber operations, or threat actors.

1 “(10) Identify information and intelligence gaps
2 related to cybersecurity risks, cybersecurity threats,
3 active malicious cyber operations, and threat actors.

4 “(11) Such other activities as the Director de-
5 termines appropriate to enhance the Agency’s ability
6 to carry out its mission as described in subsection
7 (a).

8 “(c) CHARTER.—

9 “(1) IN GENERAL.—The Collaborative shall op-
10 erate pursuant to a charter, to be developed by the
11 Director, that includes a description of each of the
12 following:

13 “(A) The organization and structure of the
14 Collaborative, as well as the relationship be-
15 tween the Collaborative and existing Agency in-
16 formation sharing functions, such programs
17 within the national cybersecurity and commu-
18 nications integration center established pursu-
19 ant to section 2209, and the manner in which
20 the Collaborative will engage, coordinate with,
21 and support other Agency divisions and pro-
22 grams.

23 “(B) The core capabilities the Collabo-
24 rative will provide.

1 “(C) How the Collaborative will prioritize,
2 refine, develop, and mature existing and future
3 capabilities to address significant, emergent, or
4 evolving cybersecurity risks, cybersecurity
5 threats, active malicious cyber operations, and
6 incidents.

7 “(D) The policies and procedures that will
8 be used to govern the Collaborative, including
9 mechanisms and protocols to improve stake-
10 holder awareness of, and input into, Collabo-
11 rative activities, as well as procedures for noti-
12 fying Collaborative partners about changes in
13 membership.

14 “(E) Policies governing the collection, use,
15 dissemination, and retention of information re-
16 lating to cybersecurity threats provided to or
17 developed by the Collaborative, consistent with
18 the protections established in sections 105 and
19 106 of the Cybersecurity Act of 2015 (6 U.S.C.
20 1504 and 1505; enacted as division N of the
21 Consolidated Appropriations Act, 2016 (Public
22 Law 114–113)).

23 “(F) Criteria to be used in selecting focus
24 areas, activities, and initiatives the Collabo-
25 rative will pursue, with procedures requiring

1 new initiatives to cite relevant portions of the
2 Charter, relevant criteria, and other factors
3 used to support such selection.

4 “(G) A description of the types or cat-
5 egories of partnerships in which the Collabo-
6 rative will engage.

7 “(H) Procedures governing the selection of
8 partner organizations and terms of such part-
9 nerships, including the following:

10 “(i) The different partnership models
11 the Collaborative plans to offer, depending
12 on the type of potential partner an organi-
13 zation is, the role and function of a poten-
14 tial partner organization within the cyber
15 ecosystem, the type of expertise and situa-
16 tional awareness a potential partner orga-
17 nization is able to provide, and the type of
18 support or information sharing a potential
19 partner organization is seeking from such
20 a partnership.

21 “(ii) The criteria to be used in the se-
22 lection of governmental and non-govern-
23 mental entities with which the Collabo-
24 rative will partner.

1 “(iii) A clearly defined process for any
2 prospective partner to apply to join the
3 Collaborative, which shall be posted on the
4 Agency’s website.

5 “(iv) A process for evaluating foreign
6 entity participation.

7 “(v) A process for alerting Collabo-
8 rative partners of new partners, including
9 foreign entities.

10 “(H) Administrative management policies
11 to facilitate regular communication between the
12 Collaborative and its partners, including desig-
13 nating Collaborative liaisons to support the ad-
14 ministrative needs of Collaborative partners.

15 “(I) The types of assessments, guidance,
16 reports, and other products the Collective will
17 release to partners and the public, as well as
18 the anticipated frequency with which such prod-
19 ucts will be published.

20 “(J) Performance metrics that will be used
21 evaluate the effectiveness of the Collaborative
22 and its activities, and track progress on specific
23 focus areas and initiatives.

1 “(2) CONSIDERATIONS.—In developing the
2 charter described in paragraph (1), the Director
3 shall consider the following:

4 “(A) Building and maintaining trust with
5 and among partners of the Collaborative.

6 “(B) Costs to partners associated with
7 participation in the Collaborative.

8 “(C) The potential of the Collaborative’s
9 activities to reduce cybersecurity risks and cy-
10 bersecurity threats to, or active malicious cyber
11 operations targeting, partners of the Collabo-
12 rative, and entities that are not partners of the
13 Collaborative.

14 “(D) Appropriate mechanisms to assess
15 collaboration with foreign entities or foreign-
16 owned entities.

17 “(d) ADVISORY COUNCIL.—Not later than 60 days
18 after the date of the enactment of this paragraph, the Di-
19 rector shall establish a Joint Cyber Defense Collaborative
20 Advisory Council, comprised of 25 representatives of Col-
21 laborative partners with diverse cybersecurity and critical
22 infrastructure roles, expertise, and situational awareness,
23 to inform the development of the charter described in
24 paragraph (1) (and any updates thereto) and provide rec-
25 ommendations on initiatives for the Collaborative to un-

1 dertake. The Director shall seek such recommendations
2 from partners of the Collaborative, and appoint members
3 to the Advisory Council, on a rotational basis, for a period
4 of not more than two years. No Member of the Cybersecu-
5 rity Advisory Committee under section 2219 may serve on
6 the Advisory Council.

7 “(e) PARTNER ORGANIZATION VIEWS.—The Director
8 shall establish a mechanism to receive the views of partner
9 organizations regarding the activities of the Collaborative,
10 and, in addition, accept voluntary annual evaluations from
11 sector coordinating councils with members that are part-
12 ners of the Collaborative. Any such evaluations shall by
13 shared by the Director with the Committee on Homeland
14 Security of the House of Representatives and the Com-
15 mittee on Homeland Security and Governmental Affairs
16 of the Senate.

17 “(f) NO RIGHT OR BENEFIT.—

18 “(1) IN GENERAL.—The provision of assistance
19 or information to, and inclusion in the Collaborative,
20 or any activity of the Collaborative, of any govern-
21 mental or non-governmental entity under this section
22 shall be at the discretion of the Director.

23 “(2) LIMITATION.—The provision of certain as-
24 sistance or information to, or inclusion in the Col-
25 laborative, or any activity of the Collaborative, pur-

1 suant to this section shall not create a right or ben-
2 efit, whether substantive or procedural, to similar
3 assistance or information for any other govern-
4 mental or non-governmental entity.

5 “(g) IMPLEMENTATION.—For any action taken to
6 implement this section, the following shall not apply:

7 “(1) Chapter 35 of title 44, United States
8 Code.

9 “(2) Chapter 10 of title 5, United States
10 Code.”;

11 (5) in subsection (g), as so redesignated—

12 (A) in the matter preceding paragraph (1),
13 by striking “Office” and inserting “Collabo-
14 rative”;

15 (B) in paragraph (1), by striking “plan-
16 ning”; and

17 (C) in paragraph (2)—

18 (i) in subparagraph (E), by striking
19 “and” after the semicolon; and

20 (ii) in subparagraph (F), by striking
21 the period and inserting a semicolon; and

22 (iii) by adding at the end the fol-
23 lowing new subparagraphs:

24 “(G) the Department of State; and

25 “(H) the Central Intelligence Agency.”;

1 (6) in subsection (h), as so redesignated, in the
2 matter preceding paragraph (1), by striking “re-
3 sponsibilities” and inserting “functions”;

4 (7) in subsection (i), as so redesignated, by
5 striking “subsection (e)” and inserting “subsection
6 (g)”;

7 (8) by adding at the end the following new sub-
8 section:

9 “(k) SUNSET.—This section shall expire on the date
10 that is five years after the date of the enactment of this
11 subsection.”.

12 (b) STRATEGY; ANNUAL BRIEFINGS; INFORMATION
13 POLICY.—

14 (1) CHARTER.—Not later than 120 days after
15 the date of the enactment of this Act, the Director
16 of the Cybersecurity and Infrastructure Security
17 Agency of the Department of Homeland Security
18 shall submit to the Committee on Homeland Secu-
19 rity of the House of Representatives and the Com-
20 mittee on Homeland Security and Governmental Af-
21 fairs of the Senate the charter for the Joint Cyber
22 Defense Collaborative developed pursuant to sub-
23 section (c) of section 2216 of the Homeland Security
24 Act of 2002 (6 U.S.C. 665b), as amended by this
25 section, and shall make such charter publicly avail-

1 able in the Federal Register within seven days after
2 such submission to Congress.

3 (2) STRATEGY.—Not later than one year after
4 the date of the enactment of this Act, the Director
5 of the Cybersecurity and Infrastructure Security
6 Agency of the Department of Homeland Security
7 shall submit to the Committee on Homeland Secu-
8 rity of the House of Representatives and the Com-
9 mittee on Homeland Security and Governmental Af-
10 fairs of the Senate a strategy describing the key pri-
11 orities, objectives, and milestones of the Joint Cyber
12 Defense Collaborative under section 2216 of the
13 Homeland Security Act of 2002 (6 U.S.C. 665b), as
14 amended by this section, as well as plans to carry
15 out such objectives and metrics that will be used to
16 evaluate effectiveness and sustain operations over
17 time. The Director may, as appropriate, submit to
18 such Committees any legislative proposals for new
19 authorities the Collaborative needs to carry out its
20 mission.

21 (3) ANNUAL BRIEFINGS.—Not later than one
22 year after the date of the enactment of this Act and
23 annually thereafter, the Director of the Cybersecu-
24 rity and Infrastructure Security Agency of the De-
25 partment of Homeland Security shall provide to the

1 Committee on Homeland Security of the House of
2 Representatives and the Committee on Homeland
3 Security and Governmental Affairs of the Senate a
4 briefing on the activities of the Joint Cyber Defense
5 Collaborative under section 2216 of the Homeland
6 Security Act of 2002 (6 U.S.C. 665b), as amended
7 by this section.

8 (4) INFORMATION ACCESS AND SECURITY POL-
9 ICY.—Not later than 90 days after the date of the
10 enactment of this Act, the Director of the Cyberse-
11 curity and Infrastructure Security Agency of the De-
12 partment of Homeland Security shall issue a policy
13 regarding how information shared with the Joint
14 Cyber Defense Collaborative under section 2216 of
15 the Homeland Security Act of 2002 (6 U.S.C.
16 665b), as amended by this section, may be used, in-
17 cluding among different participants within the Col-
18 laborative, as well as restrictions on the use of infor-
19 mation, including prohibitions on sharing informa-
20 tion with governmental and non-governmental enti-
21 ties based in or controlled by countries the intel-
22 ligence community (as such term is defined in sec-
23 tion 3(4) of the National Security Act of 1947 (50
24 U.S.C. 3003(4)) has identified as a foreign adver-
25 sary in its most recent Annual Threat Assessment or

1 that the Secretary of Homeland Security, in coordi-
2 nation with the Director of National Intelligence,
3 has identified as a foreign adversary in its most re-
4 cent Annual Threat Assessment. Such policy shall
5 also describe how information retained by the Col-
6 laborative will be secured, including that all informa-
7 tion relating to cybersecurity threats and incidents
8 (as such terms are defined in section 2200 of the
9 Homeland Security Act of 2002 (6 U.S.C. 650))
10 provided by any government or non-government par-
11 ticipant shall be protected as a High Value Asset as
12 described in Federal Information Processing Stand-
13 ards Publication 199, or any successor document.

14 (c) CLERICAL AMENDMENT.—The table of contents
15 in section 1(b) of the Homeland Security Act of 2002 is
16 amended by amending the item relating to section 2216
17 to read as follows:

“Sec. 2216. Joint Cyber Defense Collaborative.”.