.....

(Original Signature of Member)

118TH CONGRESS
2D SESSION

H. R. 9768

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.

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 ''Joint Cyber Defense Collaborative Act''.

SEC. 2. ESTABLISHMENT OF JOINT CYBER DEFENSE COLLABORATIVE.

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

(1) in the section heading, by striking ''**JOINT CYBER PLANNING OFFICE**'' and inserting ''**JOINT CYBER DEFENSE COLLABORATIVE**'';

(2) by striking subsection (a);

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

(4) by inserting before subsection (f), as so redesignated, the following new subsections:

''(a) IN GENERAL.—The Agency shall maintain the 'Joint Cyber Defense Collaborative' program (in this section referred to as the 'Collaborative') to support enhanced public-private partnerships across critical infrastructure sectors for collective cyber defense operations, information sharing, and operational collaboration, and develop, for Federal and non-Federal entities, plans for cyber defense operations, including the development of a set of coordinated actions to detect, prevent, limit, prepare for, mitigate, protect against, respond to, recover from, and build resilience to cybersecurity risks, security vulnerabilities, and incidents, and cybersecurity threats to, and incidents or active malicious cyber operations targeting, critical infrastructure or national interests. The Collaborative shall

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

''(b) FUNCTIONS.—The Collaborative shall carry out the following:

''(1) Maintain strategic, operational partnerships with entities and organizations with diverse cybersecurity roles, expertise, and situational awareness that will enhance the Agency's situational awareness of cybersecurity risks, cybersecurity threats, and active malicious cyber operations, including with cybersecurity and technology companies, critical infrastructure owners and operators, security researchers and academic institutions, nongovernmental organizations, information system vendors, manufacturers, and foreign government entities in accordance with subsection (c), and other entities as appropriate.

''(2) Develop, for public and private sector entities, plans for cyber defense operations, including the development of a set of coordinated actions to support governmental and non-governmental entities to—

''(A) protect, detect, respond to, and recover from cybersecurity risks, cybersecurity

threats, active malicious cyber operations, or incidents; or

''(B) limit, mitigate, or defend against active or anticipated malicious cyber operations that pose a potential risk to critical infrastructure or national security interests.

''(3) Develop plans for governmental and non-governmental entities, including cyber incident response plans under 2210(c), plans relating to threat-focused campaigns, and plans to address long-term cybersecurity priorities.

''(4) Gather, analyze, synthesize, and rapidly share information relating to cybersecurity threats and warnings to inform collective cyber defense operations, either through direct engagement or through the sharing of cybersecurity guidance through industry organizations to drive action across all stakeholder communities.

''(5) Facilitate the development and publication of joint analyses with Government and non-government partners, as well as international partners, as appropriate, regarding threat actors, cybersecurity risks, cybersecurity threats, active malicious cyber operations, and incidents within and across critical infrastructure sectors, to enhance awareness of ad-

versary tactics, techniques, and procedures and provide recommendations for mitigation.

''(6) Utilizing mechanisms that enable confidential real-time information sharing and dissemination of technical products between the Collaborative and its partners.

''(7) Develop processes and procedures to rapidly share with non-governmental entities timely and actionable cyber threat intelligence and information from Government entities, including the Collaborative's partners, for purposes of informing joint activities within the Collaborative, as well as proactive defense actions to defend critical infrastructure and non-Federal networks.

''(8) Establish, as appropriate, focused initiatives designed to respond to significant, emergent, or evolving cybersecurity risks or cybersecurity threats to, or active malicious cyber operations targeting, critical infrastructure sectors or technologies, including industrial control systems.

''(9) Develop plans for cyber defense operations for Federal Government and non-Federal Government entities, as well as plans to respond to specific cybersecurity risks, cybersecurity threats, active malicious cyber operations, or threat actors.

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

"(11) Such other activities as the Director determines appropriate to enhance the Agency's ability to carry out its mission as described in subsection (a).

"(c) CHARTER.—

"(1) IN GENERAL.—The Collaborative shall operate pursuant to a charter, to be developed by the Director, that includes a description of each of the following:

"(A) The organization and structure of the Collaborative, as well as the relationship between the Collaborative and existing Agency information sharing functions, such programs within the national cybersecurity and communications integration center established pursuant to section 2209, and the manner in which the Collaborative will engage, coordinate with, and support other Agency divisions and programs.

"(B) The core capabilities the Collaborative will provide.

"(C) How the Collaborative will prioritize, refine, develop, and mature existing and future capabilities to address significant, emergent, or evolving cybersecurity risks, cybersecurity threats, active malicious cyber operations, and incidents.

"(D) The policies and procedures that will be used to govern the Collaborative, including mechanisms and protocols to improve stakeholder awareness of, and input into, Collaborative activities, as well as procedures for notifying Collaborative partners about changes in membership.

"(E) Policies governing the collection, use, dissemination, and retention of information relating to cybersecurity threats provided to or developed by the Collaborative, consistent with the protections established in sections 105 and 106 of the Cybersecurity Act of 2015 (6 U.S.C. 1504 and 1505; enacted as division N of the Consolidated Appropriations Act, 2016 (Public Law 114–113)).

"(F) Criteria to be used in selecting focus areas, activities, and initiatives the Collaborative will pursue, with procedures requiring

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

"(G) A description of the types or categories of partnerships in which the Collaborative will engage.

"(H) Procedures governing the selection of partner organizations and terms of such partnerships, including the following:

"(i) The different partnership models the Collaborative plans to offer, depending on the type of potential partner an organization is, the role and function of a potential partner organization within the cyber ecosystem, the type of expertise and situational awareness a potential partner organization is able to provide, and the type of support or information sharing a potential partner organization is seeking from such a partnership.

"(ii) The criteria to be used in the selection of governmental and non-governmental entities with which the Collaborative will partner.

"(iii) A clearly defined process for any prospective partner to apply to join the Collaborative, which shall be posted on the Agency's website.

"(iv) A process for evaluating foreign entity participation.

"(v) A process for alerting Collaborative partners of new partners, including foreign entities.

"(H) Administrative management policies to facilitate regular communication between the Collaborative and its partners, including designating Collaborative liaisons to support the administrative needs of Collaborative partners.

"(I) The types of assessments, guidance, reports, and other products the Collective will release to partners and the public, as well as the anticipated frequency with which such products will be published.

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

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

"(A) Building and maintaining trust with and among partners of the Collaborative.

"(B) Costs to partners associated with participation in the Collaborative.

"(C) The potential of the Collaborative's activities to reduce cybersecurity risks and cybersecurity threats to, or active malicious cyber operations targeting, partners of the Collaborative, and entities that are not partners of the Collaborative.

"(D) Appropriate mechanisms to assess collaboration with foreign entities or foreign-owned entities.

"(d) ADVISORY COUNCIL.—Not later than 60 days after the date of the enactment of this paragraph, the Director shall establish a Joint Cyber Defense Collaborative Advisory Council, comprised of 25 representatives of Collaborative partners with diverse cybersecurity and critical infrastructure roles, expertise, and situational awareness, to inform the development of the charter described in paragraph (1) (and any updates thereto) and provide recommendations on initiatives for the Collaborative to un-

dertake. The Director shall seek such recommendations from partners of the Collaborative, and appoint members to the Advisory Council, on a rotational basis, for a period of not more than two years. No Member of the Cybersecurity Advisory Committee under section 2219 may serve on the Advisory Council.

''(e) PARTNER ORGANIZATION VIEWS.—The Director shall establish a mechanism to receive the views of partner organizations regarding the activities of the Collaborative, and, in addition, accept voluntary annual evaluations from sector coordinating councils with members that are partners of the Collaborative. Any such evaluations shall by shared by the Director with the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate.

''(f) NO RIGHT OR BENEFIT.—

''(1) IN GENERAL.—The provision of assistance or information to, and inclusion in the Collaborative, or any activity of the Collaborative, of any governmental or non-governmental entity under this section shall be at the discretion of the Director.

''(2) LIMITATION.—The provision of certain assistance or information to, or inclusion in the Collaborative, or any activity of the Collaborative, pur-

suant to this section shall not create a right or benefit, whether substantive or procedural, to similar assistance or information for any other governmental or non-governmental entity.

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

''(1) Chapter 35 of title 44, United States Code.

''(2) Chapter 10 of title 5, United States Code.'';

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

(A) in the matter preceding paragraph (1), by striking ''Office'' and inserting ''Collaborative'';

(B) in paragraph (1), by striking ''planning''; and

(C) in paragraph (2)—

(i) in subparagraph (E), by striking ''and'' after the semicolon; and

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

(iii) by adding at the end the following new subparagraphs:

''(G) the Department of State; and

''(H) the Central Intelligence Agency.'';

(6) in subsection (h), as so redesignated, in the matter preceding paragraph (1), by striking ''responsibilities'' and inserting ''functions'';

(7) in subsection (i), as so redesignated, by striking ''subsection (c)'' and inserting ''subsection (g)''; and

(8) by adding at the end the following new subsection:

''(k) SUNSET.—This section shall expire on the date that is five years after the date of the enactment of this subsection.''.

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

(1) CHARTER.—Not later than 120 days after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate the charter for the Joint Cyber Defense Collaborative developed pursuant to subsection (c) of section 2216 of the Homeland Security Act of 2002 (6 U.S.C. 665b), as amended by this section, and shall make such charter publicly avail-

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

(2) STRATEGY.—Not later than one year after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall submit to the Committee on Homeland Security of the House of Representatives and the Committee on Homeland Security and Governmental Affairs of the Senate a strategy describing the key priorities, objectives, and milestones of the Joint Cyber Defense Collaborative under section 2216 of the Homeland Security Act of 2002 (6 U.S.C. 665b), as amended by this section, as well as plans to carry out such objectives and metrics that will be used to evaluate effectiveness and sustain operations over time. The Director may, as appropriate, submit to such Committees any legislative proposals for new authorities the Collaborative needs to carry out its mission.

(3) ANNUAL BRIEFINGS.—Not later than one year after the date of the enactment of this Act and annually thereafter, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall provide to the

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

(4) INFORMATION ACCESS AND SECURITY POLICY.—Not later than 90 days after the date of the enactment of this Act, the Director of the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security shall issue a policy regarding how information shared with the Joint Cyber Defense Collaborative under section 2216 of the Homeland Security Act of 2002 (6 U.S.C. 665b), as amended by this section, may be used, including among different participants within the Collaborative, as well as restrictions on the use of information, including prohibitions on sharing information with governmental and non-governmental entities based in or controlled by countries the intelligence community (as such term is defined in section 3(4) of the National Security Act of 1947 (50 U.S.C. 3003(4)) has identified as a foreign adversary in its most recent Annual Threat Assessment or

that the Secretary of Homeland Security, in coordination with the Director of National Intelligence, has identified as a foreign adversary in its most recent Annual Threat Assessment. Such policy shall also describe how information retained by the Collaborative will be secured, including that all information relating to cybersecurity threats and incidents (as such terms are defined in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650)) provided by any government or non-government participant shall be protected as a High Value Asset as described in Federal Information Processing Standards Publication 199, or any successor document.

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

"Sec. 2216. Joint Cyber Defense Collaborative.".