

CYBERSECURITY ADVISORY COMMITTEE
AUTHORIZATION ACT OF 2020

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

TO ACCOMPANY

S. 4024

TO ESTABLISH IN THE CYBERSECURITY AND INFRASTRUCTURE
SECURITY AGENCY OF THE DEPARTMENT OF HOMELAND
SECURITY A CYBERSECURITY ADVISORY COMMITTEE



SEPTEMBER 9, 2020.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

RON JOHNSON, Wisconsin, *Chairman*

ROB PORTMAN, Ohio
RAND PAUL, Kentucky
JAMES LANKFORD, Oklahoma
MITT ROMNEY, Utah
RICK SCOTT, Florida
MICHAEL B. ENZI, Wyoming
JOSH HAWLEY, Missouri

GARY C. PETERS, Michigan
THOMAS R. CARPER, Delaware
MAGGIE HASSAN, New Hampshire
KAMALA D. HARRIS, California
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

GABRIELLE D'ADAMO SINGER, *Staff Director*

JOSEPH C. FOLIO III, *Chief Counsel*

MICHAEL J.R. FLYNN, *Senior Counsel*

ANDREW J. TIMM, *Professional Staff Member*

DAVID M. WEINBERG, *Minority Staff Director*

ZACHARY I. SCHRAM, *Minority Chief Counsel*

JEFFREY D. ROTHBLUM, *Minority Senior Professional Staff Member*

LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 528

116th CONGRESS }
2d Session }

SENATE

{ REPORT
{ 116-265

CYBERSECURITY ADVISORY COMMITTEE AUTHORIZATION
ACT OF 2020

SEPTEMBER 9, 2020.—Ordered to be printed

Mr. JOHNSON, from the Committee on Homeland Security and
Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 4024]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 4024) to establish in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security a Cybersecurity Advisory Committee, and for other purposes, having considered the same, reports favorably thereon with an amendment in the nature of a substitute and recommends that the bill, as amended, do pass.

CONTENTS

	Page
I. Purpose and Summary	1
II. Background and Need for the Legislation	2
III. Legislative History	3
IV. Section-by-Section Analysis	3
V. Evaluation of Regulatory Impact	5
VI. Congressional Budget Office Cost Estimate	6
VII. Changes in Existing Law Made by the Bill, as Reported	7

I. PURPOSE AND SUMMARY

The purpose of S. 4024, the Cybersecurity Advisory Committee Authorization Act of 2020, is to amend the Homeland Security Act of 2002 to establish a Cybersecurity Advisory Committee (Advisory Committee) within the Department of Homeland Security’s (DHS or the Department) Cybersecurity and Infrastructure Security Agency (CISA). The Advisory Committee is to be comprised of representatives of state and local governments as well as cybersecurity subject matter experts who would report to the Director of CISA.

The Advisory Committee would be tasked to assist CISA in the execution of its cybersecurity mission by advising, consulting with, and making recommendations to the Director of CISA concerning the development, refinement, and implementation of CISA's cybersecurity policies, programs, planning, and training. This bill will better position CISA to effectively execute its cyber mission.

II. BACKGROUND AND THE NEED FOR LEGISLATION

In September 2018, the Trump Administration released the National Cybersecurity Strategy, which underscores the Federal Government's intent to strengthen its collaboration with the private sector and non-Federal entities to combat cyber threats and secure critical infrastructure.¹ Additionally, the 2018 DHS Cybersecurity Strategy recognized the need to “partner with key stakeholders, including sector specific agencies and the private sector, to drive better cybersecurity.”²

To better position DHS to carry out its cybersecurity and infrastructure protection mission, Congress re-designated and restructured the Department's National Protection and Programs Directorate as CISA through the Cybersecurity and Infrastructure Security Agency Act of 2018.³ More specifically, Congress established CISA to, among other things, lead DHS's coordination “with partners at all levels of government, and from the private and non-profit sectors, to share information and build greater trust in order to make our cyber and physical infrastructure more secure.”⁴

CISA has demonstrated its commitment to improving its partnerships with non-Federal entities. For example, in October 2019, CISA Director Chris Krebs testified before the Committee at a hearing entitled, “Supply Chain Security, Global Competitiveness, and 5G.”⁵ When asked by Chairman Ron Johnson what Congress could do to assist CISA in achieving its goals and priorities, Director Krebs said that Congress should “[m]ake it easier for [CISA] to be able to convene groups to develop frameworks, to share more broadly.”⁶ Additionally, at a Committee hearing held in February 2020, Director Krebs testified that CISA's goal is to work with government and industry partners in order to create “a more strategic and unified approach towards improving our nation's overall defensive posture against malicious cyber activity.”⁷ At the same hearing, Director Krebs stated that as an agency, CISA's pathway to providing more value to its partners requires “listening and learning what [its non-Federal partners] actually need.”⁸

¹The White House, *National Cybersecurity Strategy* 8, (2018), available at <https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf>.

²U.S. Department of Homeland Security, *U.S. Department of Homeland Security Cybersecurity Strategy* 11 (2018), available at https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

³H. Rept. 115–454 at 2 (2017), available at <https://www.congress.gov/115/crpt/hrpt454/CRPT-115hrpt454.pdf>.

⁴*Id.*

⁵*Supply Chain Security, Global Competitiveness, and 5G: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 116th Cong. (Oct. 19, 2019), available at <https://www.govinfo.gov/content/pkg/CHRG-116shrg40385/pdf/CHRG-116shrg40385.pdf>.

⁶*Id.* (testimony of CISA Director Chris Krebs).

⁷*What States, Locals and the Business Community Should Know and Do: A Roadmap for Effective Cybersecurity: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 116th Cong. (Feb. 11, 2020) (testimony of CISA Director Chris Krebs).

⁸*Id.*

Additionally, the Cyberspace Solarium Commission (CSC), a bipartisan, bicameral commission, was established in the John S. McCain National Defense Authorization Act of 2019 to “develop a consensus on a strategic approach to defending the United States in cyberspace against cyber attacks of significant consequence.”⁹ In March 2020, the CSC published its final report, which included a broad recommendation to strengthen CISA “to promote a more secure cyber ecosystem, and to serve as the central civilian cybersecurity authority to support federal, state and local, and private sector cybersecurity efforts.”¹⁰ Specifically, the CSC recommended including a cybersecurity advisory committee for CISA to better account for non-Federal interests.¹¹

S. 4024 formally establishes an advisory body comprised of a diverse set of experts representing the private and non-Federal public sector within CISA. The bill also establishes a process to provide direct input to CISA on policies, programs, planning, and training to account for non-Federal interests, thereby enhancing CISA’s ability to engage with both public and private sector partners. The legislation should facilitate stakeholder engagement and ensure that a wide variety of views are represented, including through a geographically diverse membership.

III. LEGISLATIVE HISTORY

Senator David Perdue (R-GA) introduced S. 4024, the Cybersecurity Advisory Committee Authorization Act of 2020, on June 22, 2020, with Senator Kyrsten Sinema (D-AZ). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 4024 at a business meeting on July 22, 2020. During the business meeting, Chairman Johnson and Senator Sinema offered a substitute amendment. The amendment provided additional oversight authorities to the Director, clarified the structure and composition of the Advisory Committee and its membership, and included measures to increase transparency of the Advisory Committee and its work. The Johnson-Sinema substitute amendment was adopted by voice vote *en bloc*. The bill, as amended, was reported favorably by voice vote *en bloc*. Senators present for both the vote on the amendment and on final passage were Johnson, Portman, Paul, Lankford, Romney, Scott, Enzi, Hawley, Peters, Carper, Hassan, Harris, and Rosen.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section names the bill the “Cybersecurity Advisory Committee Authorization Act of 2020.”

Section 2. Cybersecurity Advisory Committee

Section 2, subsection (a) adds a new section, section 2215, to the Homeland Security Act of 2002 to establish the Advisory Committee within CISA.

⁹Pub. L. No. 115–232, 115th Cong. (2018).

¹⁰Cyberspace Solarium Commission 3 (Mar. 2020), available at <https://www.solarium.gov/report>.

¹¹*Id.* at 41.

New section 2215 subsection (a) establishes the Advisory Committee. Subsection (b)(1) lays out the duties of the Advisory Committee. Specifically, this subsection requires that the Advisory Committee advise, consult with, report and make recommendations to the Director of CISA on the development, refinement, and implementation of policies, programs, planning, and training pertaining to the Agency's cybersecurity mission. Subsection (b)(2) requires the Advisory Committee, at the Director's request, to develop recommendations regarding improving and advancing CISA's cybersecurity mission and strengthening the United States' cybersecurity. Recommendations made by the Advisory Committee must be approved by the Committee before the submission of an annual report.

New section 2215, subsection (b)(3) requires the Advisory Committee to submit periodic reports on matters identified by the Director as well as matters identified by a majority of the members of the Advisory Committee.

New section 2215, subsection (b)(4) requires the Advisory Committee to submit an annual report including the Advisory Committee's activities, findings, and recommendations, including those of any subcommittee established under this Act, for the preceding year. Not later than 180 days after the Director receives the Advisory Committee's annual report, the Director must publish a public version of the report. Subsection (b)(5) requires the Director of CISA to respond in writing not later than 90 days after receiving any recommendation from the Advisory Committee. If the Director concurs with the recommendation, the Director must also submit an action plan to implement the recommendation; if the Director does not concur with the recommendation, the Director must provide justification for why the recommendation will not be implemented.

New section 2215, subsection (b)(6) lays out the congressional notification process. Specifically, this subsection requires the Director of CISA to provide the Committees on Homeland Security and Governmental Affairs and Appropriations of the Senate and the Committees on Homeland Security and Appropriations of the House of Representatives a briefing on feedback from the Advisory Committee.

New section 2215, subsection (b)(7) requires the Director of CISA to establish structure and governance rules concerning the Advisory Committee and any subcommittee established under the legislation.

New section 2215, subsection (c) outlines the membership of the Advisory Committee. The Director of CISA shall appoint up to 35 individuals to serve as members of the Advisory Committee, within 180 days of the bill's enactment. The bill requires that the membership consist of subject matter experts, be geographically balanced, and include representatives from state, local, and tribal governments and a broad range of industries such as defense, education, financial services and insurance, healthcare, manufacturing, and other relevant fields identified by the Director. At least one, but not more than three, members of the Advisory Committee may represent a private sector category identified in this bill. The membership of the Advisory Committee is required to be made available on a public website at least once a year and must be updated to

reflect changes in membership when they occur. Members of the Advisory Committee are permitted to serve for a period of two years, but may also serve in a holdover capacity until a successor is appointed. The Director of CISA has the authority to remove participants at his or her discretion. Members of the Advisory Committee are prohibited from being compensated by the Federal Government for their participation. The Advisory Committee must meet at least semiannually and may convene additional meetings as necessary. At least one semiannual meeting must be open to the public, and attendance must be recorded at each meeting. Within 60 days of appointing a member to the Advisory Committee, the Director is required to determine whether that member should be restricted from reviewing, discussing, or possessing classified materials. Members of the Advisory Committee are required to protect all classified information in accordance with applicable requirements. The requirements under this bill concerning a member's access to classified materials are not to affect the security clearance held by said member. Finally, the members of the Advisory Committee are required to appoint an Advisory Committee chairperson as well as a chairperson for each subcommittee.

New section 2215, subsection (d) requires the Director of CISA to establish subcommittees within the Advisory Committee to address cybersecurity security issues, such as information exchange, critical infrastructure, risk management, and public and private partnerships. The subcommittees are required to meet not less than semiannually, and submit to the Advisory Committee information concerning its activities, findings, recommendations related to the subject matter considered by the subcommittee. The chair of the Advisory Committee must appoint members to serve on subcommittees and ensure that the appointed member possesses expertise relevant to the subcommittee's focus.

Subsection (b) of the bill adds a clerical amendment to modify the Homeland Security Act of 2002's table of contents consistent with the new section added by this legislation.

V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, August 5, 2020.

Hon. RON JOHNSON,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 4024, the Cybersecurity Advisory Committee Authorization Act of 2020.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prospero.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

S. 4024, Cybersecurity Advisory Committee Authorization Act of 2020			
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on July 22, 2020			
By Fiscal Year, Millions of Dollars	2020	2020-2025	2020-2030
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	2	not estimated
Statutory pay-as-you-go procedures apply?	No	Mandate Effects	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2031?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

S. 4024 would require the Director of the Cybersecurity and Infrastructure Security Agency (CISA) to establish an advisory committee that would be composed of members from state and local governments and the private sector. The committee would provide CISA with recommendations on the implementation of cybersecurity policies and programs.

Using information from the agency about the administrative costs of similar advisory committees, CBO estimates that staff salaries, travel costs, and other expenses would be less than \$500,000 annually. In total, implementing S. 4024 would cost \$2 million over the 2020–2025 period; such spending would be subject to the availability of appropriations.

On October 11, 2019, CBO transmitted a cost estimate for H.R. 1975, the Cybersecurity Advisory Committee Authorization Act of 2019, as ordered reported by the House Committee on Homeland Security on September 25, 2019. The two pieces of legislation are similar, and CBO's estimate of their budgetary effects is the same.

The CBO staff contact for this estimate is Aldo Proserpi. The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

In compliance with paragraph 12 of rule XXVI of the Standing Rules of the Senate, the following changes in existing law made by the bill, as reported, are shown as follows: (existing law proposed to be omitted is enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

HOMELAND SECURITY ACT OF 2002

* * * * *

Section 1. Short Title; Table of Contents.

(a) * * *

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

**TITLE XXII—CYBERSECURITY AND
INFRASTRUCTURE SECURITY AGENCY**

**Subtitle A—Cybersecurity and Infrastructure
Security**

* * * * *

Sec. 2215. Cybersecurity Advisory Committee.

* * * * *

**TITLE XXII—CYBERSECURITY AND
INFRASTRUCTURE SECURITY AGENCY**

* * * * *

**Subtitle A—Cybersecurity and Infrastructure
Security**

* * * * *

SEC. 2215. CYBERSECURITY ADVISORY COMMITTEE.

(a) *ESTABLISHMENT*.—The Secretary shall establish within the Agency a Cybersecurity Advisory Committee (referred to in this section as the “Advisory Committee”).

(b) *DUTIES*.—

(1) *IN GENERAL*.—The Advisory Committee shall advise, consult with, report to, and make recommendations to the Director, as appropriate, on the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

(2) *RECOMMENDATIONS*.—

(A) *IN GENERAL.*—The Advisory Committee shall develop, at the request of the Director, recommendations for improvements to advance the cybersecurity mission of the Agency and strengthen the cybersecurity of the United States.

(B) *RECOMMENDATIONS OF SUBCOMMITTEES.*—Recommendations agreed upon by subcommittees established under subsection (d) for any year shall be approved by the Advisory Committee before the Advisory Committee submits to the Director the annual report under paragraph (4) for that year.

(3) *PERIODIC REPORTS.*—The Advisory Committee shall periodically submit to the Director—

(A) reports on matters identified by the Director; and

(B) reports on other matters identified by a majority of the members of the Advisory Committee.

(4) *ANNUAL REPORT.*—

(A) *IN GENERAL.*—The Advisory Committee shall submit to the Director an annual report providing information on the activities, findings, and recommendations of the Advisory Committee, including its subcommittees, for the preceding year.

(B) *PUBLICATION.*—Not later than 180 days after the date on which the Director receives an annual report for a year under subparagraph (A), the Director shall publish a public version of the report describing the activities of the Advisory Committee and such related matters as would be informative to the public during that year, consistent with section 552(b) of title 5, United States Code.

(5) *FEEDBACK.*—Not later than 90 days after receiving any recommendation submitted by the Advisory Committee under paragraph (2), (3), or (4), the Director shall respond in writing to the Advisory Committee with feedback on the recommendation. Such a response shall include—

(A) with respect to any recommendation with which the Director concurs, an action plan to implement the recommendation; and

(B) with respect to any recommendation with which the Director does not concur, a justification for why the Director does not plan to implement the recommendation.

(6) *CONGRESSIONAL NOTIFICATION.*—Not less frequently than once per year after the date of enactment of this section, the Director shall provide to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security and the Committee on Appropriations of the House of Representatives a briefing on feedback from the Advisory Committee.

(7) *GOVERNANCE RULES.*—The Director shall establish rules for the structure and governance of the Advisory Committee and all subcommittees established under subsection (d).

(c) *MEMBERSHIP.*—

(1) *APPOINTMENT.*—

(A) *IN GENERAL.*—Not later than 180 days after the date of enactment of the Cybersecurity Advisory Committee Au-

thorization Act of 2020, the Director shall appoint the members of the Advisory Committee.

(B) *COMPOSITION.*—The membership of the Advisory Committee shall consist of not more than 35 individuals.

(C) *REPRESENTATION.*—

(i) *IN GENERAL.*—The membership of the Advisory Committee shall—

(I) consist of subject matter experts;

(II) be geographically balanced; and

(III) include representatives of State, local, and Tribal governments and of a broad range of industries, which may include the following:

(aa) Defense.

(bb) Education.

(cc) Financial services and insurance.

(dd) Healthcare.

(ee) Manufacturing.

(ff) Media and entertainment.

(gg) Chemicals.

(hh) Retail.

(ii) Transportation.

(jj) Energy.

(kk) Information Technology.

(ll) Communications.

(mm) Other relevant fields identified by the Director.

(ii) *PROHIBITION.*—Not less than 1 member nor more than 3 members may represent any 1 category under clause (i)(III).

(iii) *PUBLICATION OF MEMBERSHIP LIST.*—The Advisory Committee shall publish its membership list on a publicly available website not less than once per fiscal year and shall update the membership list as changes occur.

(2) *TERM OF OFFICE.*—

(A) *TERMS.*—The term of each member of the Advisory Committee shall be 2 years, except that a member may continue to serve until a successor is appointed.

(B) *REMOVAL.*—The Director may review the participation of a member of the Advisory Committee and remove such member any time at the discretion of the Director.

(C) *REAPPOINTMENT.*—A member of the Advisory Committee may be reappointed for an unlimited number of terms.

(3) *PROHIBITION OF COMPENSATION.*—The members of the Advisory Committee may not receive pay or benefits from the United States Government by reason of their service on the Advisory Committee.

(4) *MEETINGS.*—

(A) *IN GENERAL.*—The Director shall require the Advisory Committee to meet not less frequently than semiannually, and may convene additional meetings as necessary.

(B) *PUBLIC MEETINGS.*—At least one of the meetings referred to in subparagraph (A) shall be open to the public.

(C) *ATTENDANCE.*—The Advisory Committee shall maintain a record of the persons present at each meeting.

(5) *MEMBER ACCESS TO CLASSIFIED INFORMATION.*—

(A) *IN GENERAL.*—Not later than 60 days after the date on which a member is first appointed to the Advisory Committee and before the member is granted access to any classified information, the Director shall determine, for the purposes of the Advisory Committee, if the member should be restricted from reviewing, discussing, or possessing classified information.

(B) *ACCESS.*—Access to classified materials shall be managed in accordance with Executive Order No. 13526 of December 29, 2009 (75 Fed. Reg. 707), or any subsequent corresponding Executive Order.

(C) *PROTECTIONS.*—A member of the Advisory Committee shall protect all classified information in accordance with the applicable requirements for the particular level of classification of such information.

(D) *RULE OF CONSTRUCTION.*—Nothing in this paragraph shall be construed to affect the security clearance of a member of the Advisory Committee or the authority of a Federal agency to provide a member of the Advisory Committee access to classified information.

(6) *CHAIRPERSON.*—The Advisory Committee shall select, from among the members of the Advisory Committee—

(A) a member to serve as chairperson of the Advisory Committee; and

(B) a member to serve as chairperson of each subcommittee of the Advisory Committee established under subsection (d).

(d) *SUBCOMMITTEES.*—

(1) *IN GENERAL.*—The Director shall establish subcommittees within the Advisory Committee to address cybersecurity issues, which may include the following:

(A) Information exchange.

(B) Critical infrastructure.

(C) Risk management.

(D) Public and private partnerships.

(2) *MEETINGS AND REPORTING.*—Each subcommittee shall meet not less frequently than semiannually, and submit to the Advisory Committee for inclusion in the annual report required under subsection (b)(4) information, including activities, findings, and recommendations, regarding subject matter considered by the subcommittee.

(3) *SUBJECT MATTER EXPERTS.*—The chairperson of the Advisory Committee shall appoint members to subcommittees and shall ensure that each member appointed to a subcommittee has subject matter expertise relevant to the subject matter of the subcommittee.