CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY
CYBERSECURITY ADVISORY COMMITTEE
BYLAWS

I. AUTHORITY

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee is established under the *National Defense Authorization Act* for Fiscal Year 2021, P.L. 116-283 (NDAA). Pursuant to section 871(a) of the *Homeland Security Act of 2002*, 6 U.S.C. § 451(a), the Secretary of Homeland Security established the CISA Cybersecurity Advisory Committee for the purposes set forth herein. This statutory committee is established in accordance with and operates under the provisions of the *Federal Advisory Committee Act* (FACA) (5 U.S.C. Chapter 10).

II. PURPOSE

The CISA Cybersecurity Advisory Committee provides independent, strategic, and actionable consensus recommendations to the CISA Director on a range of cybersecurity issues, topics, and challenges, including, but not limited to: information exchange; critical infrastructure; risk management; and public and private partnerships. The CISA Cybersecurity Advisory Committee shall develop, at the request of the CISA Director [hereinafter referred to as the "Director"], and incorporating guidance from the Secretary of Homeland Security [hereinafter referred to as the "Secretary"], recommendations on matters related to the development, refinement, and implementation of policies, programs, planning, and training pertaining to the cybersecurity mission of the Agency.

III. MEMBERSHIP AND MEMBER RESPONSIBILITIES

1. *Composition*

   The Committee shall be composed of up to 35 members. Members are appointed by the Director. The CISA Cybersecurity Advisory Committee Designated Federal Officer (DFO) will coordinate with the DFO for the Homeland Security Advisory Council (HSAC) to ensure that appointments to the Committee do not impact the HSAC mission, member duties, or activities. In order for the Director to fully leverage broad-ranging experience and education, the CISA Cybersecurity Advisory Committee must be diverse, with regard to professional and technical expertise. The Department of Homeland Security is committed to pursuing opportunities, consistent with applicable law, to compose a committee that reflects the diversity of the nation's people. These members shall consist of subject matter experts from diverse and appropriate professions and communities nationwide, be geographically balanced, and include representatives from State, local, tribal, and territorial governments and a broad and inclusive range of industries. The Director may select members with a background in cybersecurity issues relevant to CISA policies, plans, and programs. Specifically, membership

may include representatives from the following industries recommended in the authorizing statute:

i. Defense;

ii. Education;

iii. Financial services and insurance;

iv. Healthcare;

v. Manufacturing;

vi. Media and entertainment;

vii. Chemical;

viii. Retail;

ix. Transportation;

x. Energy;

xi. Information Technology;

xii. Communications; and

xiii. Other relevant fields identified by the Director.

Members shall serve as representatives to speak on behalf of their respective organization, group, or industry.

2. *Appointment*

Members of the Committee are appointed by and serve at the pleasure of the Director. Membership is voluntary and members are not compensated for their services. Appointments are personal to the member and cannot be transferred to another individual or other employees of the member's organization of employment. Members may not designate someone to attend in their stead, participate in discussions, or vote. If a member becomes a federal employee or otherwise ineligible for membership, the member must inform the CISA Cybersecurity Advisory Committee DFO. Additionally, if it is the intent of the member to resign, he or she must submit the request in writing to the Director as well as the DFO.

3. *Terms of Office*

   Members will serve two-year terms. A member may be reappointed for an unlimited number of terms. In the event that the CISA Cybersecurity Advisory Committee terminates, all appointments to the Committee shall terminate.

4. *Security Clearances*

   Members are not required to have security clearances to participate in committee activities.

5. *Members' Responsibilities*

   Since the membership of the CISA Cybersecurity Advisory Committee is constructed to balance as many aspects and viewpoints as possible, member attendance and participation at meetings is vital to the CISA Cybersecurity Advisory Committee's mission. Members are expected to personally attend and participate in Committee meetings, to include virtual meetings. The Director may review the participation of a member of the CISA Cybersecurity Advisory Committee and remove such member any time at the discretion of the Director. The DFO will recommend to the Director that any member who is unable to fulfill his/her responsibility be removed from the Committee. Members of the CISA Cybersecurity Advisory Committee may be recommended for removal by the DFO for reasons such as, but not limited to:

   a. Consistently missing meetings or not participating in the Committee's work; and
   b. Engaging in activities that are illegal or violate the restrictions on members' activities as outlined below.

6. *Restriction on Members' Activities*

   a. Members may not use their access to the Federal Government as a member of this Committee for the purpose of soliciting business for or otherwise seeking economic advantage for themselves, their companies, or their employers. Members may not use any non-public information obtained in the course of their duties as a member for personal gain or for that of their company or employer. Members must hold any non-public information, including pre-decisional documents such as draft reports, in confidence.
   b. The Committee as a whole may advise CISA on legislation or may recommend legislative action to CISA. In their capacities as members of the CISA Cybersecurity Advisory Committee, individual members may not petition or lobby Congress for or against particular legislation or encourage others to do so.
   c. Members of the CISA Cybersecurity Advisory Committee are advisors to the agency and have no authority to speak for the Committee, CISA, or for the Department of Homeland Security

(DHS) outside of the Committee structure.

d. Members may not testify before Congress in their capacity as a member of the CISA Cybersecurity Advisory Committee. If requested to testify before Congress, members of the CISA Cybersecurity Advisory Committee:
    i. Cannot represent or speak for the Committee, CISA, DHS, or any agency or the Administration in their testimony.
    ii. Cannot provide information or comment on Committee recommendations that are not publicly available.
    iii. May state that they are a member of the Committee.
    iv. May speak to their personal observations as to their service on the Committee.
e. If speaking outside of the Committee structure at other forums or meetings, the restrictions in Section (d) also apply.

IV. OFFICIALS

1. *CISA Cybersecurity Advisory Committee Leadership*

The CISA Cybersecurity Advisory Committee will select a Chair and Vice Chair from among the Committee members through a nomination and formal vote. The Chair and Vice Chair will serve for a two-year term. The Chair and/or Vice Chair may be reappointed for additional terms, not to exceed two terms. The DFO may determine that the Chair or Vice Chair's term be extended by no more than six months, in order to complete their oversight of an outstanding task or report. If a Chair or Vice Chair is not able to serve for their entire term, an additional election will be held. The CISA Cybersecurity Advisory Committee Chair will preside at all CISA Cybersecurity Advisory Committee meetings. The Chair will conduct the meeting, provide an opportunity for participation by each member and by public attendees, ensure adherence to the agenda, maintain order, and prepare any recommendations submitted to the Agency. The Vice Chair will act as the Chair in the absence of the Chair. The Chair and Vice Chair are expected to facilitate Committee meetings and moderate all Committee deliberations. The Chair and Vice Chair will receive taskings from the Director and/or the DFO, and in coordination with the DFO, will create subcommittees to examine taskings.

2. *Designated Federal Officer*

The DFO and the Alternate DFO (ADFO) are designated by the Director. The DFO or ADFO will:

a. Coordinate with the HSAC DFO on membership considerations and study topics;
b. Approve agendas for Committee and subcommittee meetings;
c. Attend all meetings of the CISA Cybersecurity Advisory Committee to ensure the advisory activities of the Committee are within its authorized scope of responsibility;
d. Approve or call meetings of the Committee and subcommittees;

e. Adjourn meetings when such adjournment is in the public interest;
f. Chair meetings of the Committee when directed to do so by the Director or when requested in the absence of the Chair; and
g. Assist the Director in his/her reporting requirements, as outlined in Section X. This may include ensuring final Committee reports are posted on the CISA Cybersecurity Advisory Committee's publicly available website and assisting with the preparation for the Director's annual briefing to Congress.

Additionally, the DFO is responsible for assuring administrative support functions are performed, including:

a. Notifying members and for open meetings, the general public, of the time and place of each meeting;
b. Tracking all recommendations of the Committee;
c. Maintaining the record of members' attendance;
d. Preparing the minutes of all meetings of the Committee's deliberations;
e. Releasing minutes and agendas of all meetings to the general public in the manner required by law unless a specific meeting is closed to the public;
f. Attending to official correspondence;
g. Maintaining official records and filing all papers and submissions prepared for or by the Committee;
h. Developing or updating operating procedures for all Committee activities;
i. Reviewing and updating information on Committee activities in the FACA database on a monthly basis;
j. Acting as the Committee's agent to collect, validate, and pay for all vouchers for pre-approved expenditures; and
k. Preparing and handling all reports.

V. MEETING PROCEDURES

1. *Meeting Schedule and Call of Meetings*

The CISA Cybersecurity Advisory Committee will meet at least twice per year to address matters within the scope of the Committee's charter. Meetings may be held more frequently, or as necessary and appropriate, to address mission requirements. Additional meetings may be scheduled, pending approval from the DFO or ADFO. The DFO or ADFO must attend all Committee meetings.

2. *Agenda*

Meeting agendas are developed by the DFO and committee staff in coordination with the CISA Cybersecurity Advisory Committee Chair. The DFO will approve the agenda for all Committee meetings and approve the agenda for subcommittee meetings, distribute the agenda to members prior to the meeting, and will publish the agenda for Committee meetings in the Federal Register.

3. *Quorum*

A quorum of CISA Cybersecurity Advisory Committee members is the presence of fifty percent plus one of the Committee members currently appointed. A quorum of the Committee is required to vote on issues being addressed. In the event a quorum is not present, the CISA Cybersecurity Advisory Committee may conduct business that does not require a vote or decision among members. Votes will be deferred until such a time that a quorum is present.

4. *Voting Procedures*

Members will review recommendations and reports from the CISA Cybersecurity Advisory Committee subcommittees. Any item being presented to the Committee for approval must be made available to the public in advance of a Committee meeting, must be discussed by the Committee during the meeting, and must receive a majority vote from the Committee.
When a decision or recommendation of the CISA Cybersecurity Advisory Committee is required, the Chair will request a motion for a vote. A motion is considered to have been adopted if agreed to by a simple majority of a quorum of CISA Cybersecurity Advisory Committee members. Only members present at the meeting may vote on an item under consideration. No proxy votes or votes by email will be allowed.

5. *Minutes*

The DFO will prepare the minutes of each meeting and distribute copies to each Committee member. Minutes of open meetings will be available to the public on the CISA Cybersecurity Advisory Committee website. The minutes will include a record of:

a. The time, date, and place of the meeting;
b. A list of all attendees, including Committee members, staff, agency employees, and members of the public who presented oral or written statements;
c. An accurate description of each matter discussed and the resolution, if any, made by the Committee; and
d. An accurate description of public participation, including oral and written statements provided.

Minutes of closed meetings will also be available to the public upon request, subject to the withholding of matters about which public disclosure would be harmful to the interests of the Government, industry, or others, and which are exempt from disclosure under the *Freedom of Information Act* (5 U.S.C. § 552). The DFO ensures that the Chair certifies the minutes within 90 calendar days of the meeting to which they relate.

6. *Open Meetings*

The CISA Cybersecurity Advisory Committee is required to hold at least one

public meeting per year. All meetings of the CISA Cybersecurity Advisory Committee will be published in the Federal Register at least fifteen calendar days before the meeting. Members of the public may attend any meeting or portion of a meeting that is not closed to the public and may, at the determination of the DFO, offer oral comment at such meeting. Oral comments should be allowed unless it is clearly inappropriate to do so. Members of the public may submit written comments to the CISA Cybersecurity Advisory Committee. All materials provided to the committee shall be available to the public when they are provided to the members. Such materials, including any submissions by members of the public, are part of the meeting record.

7. *Closed Meetings*

Due to the sensitive nature of topics discussed, CISA Cybersecurity Advisory Committee meetings may be closed, or partially closed, in accordance with applicable law. A determination must be made by the CISA Director in accordance with DHS policy and directives that the meeting should be closed in accordance with subsection (c) of section 552b of title 5. Where the DFO has determined in advance that discussion during a committee meeting will involve matters about which public disclosure would be harmful to the interests of the Government, industry, or others, an advance notice of a closed meeting, citing the applicable exemptions of the Government in the Sunshine Act, will be published in the Federal Register. The notice may announce the closing of all or part of a meeting. If, during the course of an open meeting, matters inappropriate for public disclosure arise during discussions, the DFO or the CISA Cybersecurity Advisory Committee Chair will order such discussion to cease and will schedule it for a future committee meeting that will be approved for closure. No meeting or portion of a meeting may be closed without prior approval and notice published in the Federal Register at least 15 calendar days in advance. Closed meetings may only be attended by the DFO, Committee members, CISA and CISA Cybersecurity Advisory Committee staff, and appropriate Federal Government officials invited to provide subject matter expertise related to agenda items.

Presenters must leave immediately after giving their presentations and answering any questions. Meetings may be opened by the CISA Cybersecurity Advisory Committee DFO or ADFO after consultation with participating leadership.

VI. EXPENSES AND REIMBURSEMENTS

CISA is responsible for providing financial and administrative support to the CISA Cybersecurity Advisory Committee. Members of the CISA Cybersecurity Advisory Committee will serve on the Committee without compensation. However, to the extent permitted by law, members may be reimbursed for travel and per diem expenses if funding is available. Travel expenditures must be approved by the DFO in advance. CISA will be responsible for processing travel reimbursements for the CISA Cybersecurity Advisory Committee.

VII. ADMINISTRATION

CISA will provide administrative and clerical support to the Committee and assist in carrying out the administrative functions of the DFO as outlined in Article IV, Section 2.

VIII. SUBCOMMITTEES

The Director will establish subcommittees, as necessary. The DFO will coordinate with the HSAC DFO to ensure that subcommittees are established in such a manner as to minimize duplication and ensure complementary work activities between both groups. Subcommittee members may be composed in part or in whole of individuals who are not CISA Cybersecurity Advisory Committee members and are invited to serve the Committee by the CISA Cybersecurity Advisory Committee Chair. Subcommittees will be stood up as needed and terminate when the work is complete. The CISA Cybersecurity Advisory Committee members will consult with the DFO to determine the appropriate participants for each tasking.

1. *Subcommittee Leadership*

   CISA Cybersecurity Advisory Committee members shall select from among the members of the Committee, a member to serve as chairperson of each subcommittee.

2. *Subcommittee Members*

   The CISA Cybersecurity Advisory Committee Chair 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.

   Subcommittee members who are not members of the parent committee must sign a non-disclosure agreement and gratuitous services agreement form upon appointment.

   A subcommittee member's term of service will expire when the tasking is completed. Subcommittee members will reflect balanced viewpoints on the subject matter. All subcommittee discussions and materials, including briefings, outlines, and reports, are considered pre-decisional working drafts and shall not be publicly available. Once the tasking has been examined by a subcommittee, the subcommittee must present its work to the CISA Cybersecurity Advisory Committee for full deliberation and discussion. Reports and other materials presented to the parent committee must be publicly available.

3. *Meetings and Reporting*

   Each subcommittee shall meet not less frequently than semi-annually. In addition to supporting taskings required by the Director, the subcommittee must also provide the CISA Cybersecurity Advisory Committee with information regarding its activities, findings, and recommendations for inclusion in the annual report.

IX. RECORDKEEPING

The DFO maintains all records of the CISA Cybersecurity Advisory Committee and its subcommittees in accordance with the General Records Schedule 6.2. These records shall be available for public inspection and copying, in accordance with the *Freedom of Information Act* (5 U.S.C. § 552). All documents, reports, or other materials presented to, or prepared by or for the Committee, constitute official government records and are available to the public upon request.

X. RECOMMENDATIONS AND REPORTING

The CISA Cybersecurity Advisory Committee shall submit to the Director reports on matters identified by the Director. The subcommittee assigned to a specific tasking will present the CISA Cybersecurity Advisory Committee with a draft report for the members to deliberate, discuss, and vote upon. Once the members agree on the final product, the product, in the form of a written report, will be transmitted to the Director within 14 days of the members approving it. Once received, the Director has 90 days to respond, in writing, to the Committee with feedback on the recommendations. If the Director concurs with the recommendation, the response should include an action plan to implement the recommendation. If the Director does not concur with a recommendation, the response should include a justification as to why the Director does not plan to implement the recommendation.

Additionally, the CISA Cybersecurity Advisory Committee shall submit to the Director, with a copy to the Secretary, an annual report providing information on the activities, findings, and recommendations of the CISA Cybersecurity Advisory Committee, including its subcommittees, for the preceding year. Not later than 180 days after the date on which the Director receives an annual report for a year, the Director shall publish a public version of the report describing the activities of the CISA Cybersecurity 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. The Director will also be required to provide a briefing on feedback from the CISA Cybersecurity Advisory Committee to the Committee on Homeland Security and Governmental Affairs and the Committee on Appropriations of the Senate and the Committee on Homeland Security, the Committee on Energy and Commerce, and the Committee on Appropriations of the House of Representatives.

XI. BYLAWS APPROVAL AND AMENDMENTS

The DFO may amend these bylaws at any time, and the amendments shall become effective immediately.

Megan Tsuyi November 27, 2023

Name Date

CISA Cybersecurity Advisory Committee Designated Federal Officer