UNITED STATES DEPARTMENT OF HOMELAND SECURITY
CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL
2024 CHARTER

1. Official Designation:

Critical Infrastructure Partnership Advisory Council (CIPAC)

2. Authority:

Consistent with the Homeland Security Act of 2002(the "Act"), 6 U.S.C. § 101 *et. seq.*, including sections 871(a) and 2202 of the Act, 6 U.S.C. §§ 451(a), 652, the Secretary of Homeland Security (hereinafter referred to as the "Secretary") hereby establishes the Critical Infrastructure Partnership Advisory Council (CIPAC) for the purposes set forth herein. In recognition of the sensitive nature of the subject matter involved in CIPAC's activities, the Secretary hereby exercises the authority in section 871(a) of the Act to establish CIPAC and exempt CIPAC activities conducted pursuant to this Charter from *The Federal Advisory Committee Act* (FACA), (Title 5, United States Code, ch. 10).

3. Objectives and Scope of Activities:

CIPAC is aligned with and supports the implementation of the National Infrastructure Protection Plan: *Partnering for Critical Infrastructure Security and Resilience,* and other relevant authorities such as the *National Security Memorandum on Critical Infrastructure Security and Resilience* (NSM-22), to effectuate the interests of the partnership structure set forth in the National Infrastructure Protection Plan, or any subsequently dated issuances thereof, by coordinating federal cyber and infrastructure security and resilience programs with the cyber and infrastructure security and resilience activities of the private sector and of state, local, tribal, and territorial governments. CIPAC also operates consistent with the Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency's (CISA) work to engage Sector Risk Management Agencies (SRMAs) and critical infrastructure sector partners through the partnership structure, supporting CISA's responsibilities as the National Coordinator for critical infrastructure security and resilience. Specifically, CIPAC facilitates engagements between government representatives at the federal, state, local, tribal, and territorial levels and representatives from critical infrastructure owners and operators in each critical infrastructure sector and subsector to conduct deliberations and form consensus positions to assist the federal government.

4. Descriptions of Duties:

The duties of CIPAC are solely advisory in nature.

5. Official to Whom the Council Reports:

CIPAC may develop advice and recommendations on cyber and critical infrastructure security and resilience matters and provide them to the entities listed below. CIPAC has no authority to establish federal policy or undertake inherently governmental functions.

A. DHS;

B. The Sector Risk Management Agency (SRMA) for each sector; and

C. Other federal departments and agencies supporting the critical infrastructure security and resilience mission under the National Infrastructure Protection Plan, or any subsequently dated issuances thereof, which have responsibility for establishing and implementing federal policy and managing federal programs.

Government entities in receipt of advice, recommendations, and/or other work products developed under the auspices of CIPAC should provide a record to the CIPAC Designated Federal Officer (DFO) who serves as the responsible DHS official for the council.

6. Agency Responsible for Providing Necessary Support:
CISA will be designated as the CIPAC Executive Secretariat. The CISA Director shall be responsible for providing financial and administrative support to the CIPAC.

7. Estimated Cost, Compensation, and Staff Support:

Subject to the availability of appropriations, CISA envisions the need for, and shall provide CIPAC, funding for federal and contractor administrative support and other support equivalent to at least five (5) full-time federal employees plus an estimated annual operating cost of $1,100,000 for such funds as may be necessary to cover operating expenses and administrative costs generated in conducting its business. CIPAC members shall customarily bear their own costs of participating in CIPAC; however, CISA may pay reasonable travel expenses and per diem consistent with DHS policies and procedures, laws, and government ethics rules and guidance, and subject to the availability of funds. This annual operating cost estimate incorporates operating expenses and administrative costs, but excludes other potential costs, such as invitational travel.

CIPAC Executive Secretariat may accept the offer of another federal agency to host and provide secretariat meeting support for any CIPAC meeting they are conducting as the SRMA; the costs of such services will be borne by the offering agency and will follow CIPAC meeting operational procedures as established by the CIPAC Executive Secretariat.

8. Definitions:

For the purpose of the CIPAC Charter and Bylaws, and consistent with the National Infrastructure Protection Plan, these following definitions apply:

A. **CIPAC Participant**: CIPAC participant is a collective term referring to all CIPAC member organizations and individuals representing them, as well as subject matter experts (SME). All CIPAC participants are subject to the provisions of the Charter and Bylaws when participating in CIPAC activities.

B. **Cross-Sector Councils**: CISA recognizes cross-sector councils that function under CIPAC to address emerging issues impacting critical infrastructure. Cross-sector councils work to create consensus advice for or recommendations to relevant federal agencies on cybersecurity and infrastructure security matters and therefore must comply with all provisions in the Charter, Bylaws, and any compliance procedures and guidelines issued by the CIPAC Designated Federal Officer (DFO).

C. **Cross-Sector Working Groups**: Cross-sector working groups consist of CIPAC members representing more than one designated sector or subsector and SMEs, as needed, to address the critical infrastructure needs of their respective sectors. These groups meet on a recurring basis to create consensus advice or recommendations to relevant federal agencies and therefore must comply with all the provisions in the Charter, Bylaws, and any compliance procedures and guidelines issued by the DFO. CIPAC compliant cross-sector working groups are established by the CIPAC Charter and Bylaws. Ad-hoc cross-sector groups that meet to provide consensus advice or recommendations also qualify as cross-sector working groups under the CIPAC Charter and Bylaws.

D. **Designated Federal Officer (DFO)**: The DFO or Alternate DFO (ADFO) are CISA federal employees designated by the Director of CISA. The DFO and ADFO are responsible for ensuring implementation and adherence to all compliance procedures and guidelines issued by the DFO. CIPAC meetings will only be held upon the approval of, and at the call of, the CIPAC DFO or ADFO.

E. **Compliance Liaison Official (CLO)**: A CLO is a CISA federal employee trained and annually certified by the DFO or ADFO to perform the duties of the DFO for assigned CIPAC meetings to ensure adherence to all procedures and guidelines issued by the DFO.

F. **Government Coordinating Councils (GCC)**: Chaired by the identified SRMA, the GCCs enable interagency, intergovernmental, and cross jurisdictional coordination within and across sectors. They comprise representatives from across various levels of government (federal, state, local, and tribal), as appropriate, to the operating landscape of each individual sector. GCCs coordinate with the respective Sector Coordinating Council (SCC) to address cybersecurity and infrastructure security matters affecting the sector.

G. **Sector Coordinating Councils (SCC)**: The SCCs are self-organized, self-run, and self-governed councils that enable critical infrastructure owners and operators and representative trade or equivalent associations to interact on a wide range of sector-specific strategies, policies, activities, and issues. The SCCs serve as sector policy coordination and planning entities with the responsibility of bringing together a diverse and balanced membership that can effectively collaborate with CISA, SRMAs, and related GCCs to address and advise the federal government on the entire range of cyber and critical infrastructure security and resilience activities and issues for that sector.

H. **Sector Risk Management Agency (SRMA)**: NSM-22 identifies critical infrastructure sectors and their assigned SRMAs. As the SRMA, that federal agency is responsible for the sector's GCC and day-to-day engagement and collaboration with relevant external governmental and non-governmental bodies to work to strengthen the security and resilience of the Nation's critical infrastructure in that sector.

I. **Subject Matter Expert (SME)**: A SME is an individual who: is not affiliated with a member organization of a council under CIPAC; possesses significant expertise and substantive knowledge that is greater than that of a layperson; and works in the relevant field or industry. A SME's organizational knowledge or individualized information may be used to provide technical or industry-specific information for the purposes of informing the recommendations of a working group, cross-sector working group, affiliated sub-working group(s) or SCC. SMEs may not participate in forming consensus advice or recommendations, or serve in a leadership capacity on a GCC, SCC, cross-sector council, working group, or affiliated sub-working group. An organization that is not a member of a GCC, SCC, or cross-sector council may be invited to participate on a working group, cross-sector working group, or affiliated sub-working group as an organization-level SME. Multiple representatives from an organization may participate as SMEs.

J. **Working Groups**: CIPAC compliant working groups and affiliated sub-working groups, regardless of title, consist of CIPAC members from the designated sectors or subsectors, and SMEs, as needed, to address the critical infrastructure needs of the sector. These groups have a defined purpose, pre-determined duration, and meet on a recurring basis to create consensus advice or recommendations to the relevant federal agencies and therefore must comply with all the provisions in the CIPAC Charter, Bylaws, and any compliance procedures and guidelines issued by the DFO. Ad-hoc groups that meet to provide consensus advice or recommendations also qualify as working groups under the Charter and Bylaws.

9. Designated Federal Officer:

The CISA Director shall appoint a full-time employee as the Designated Federal Officer (DFO) and Alternate DFOs (ADFO) as part of the CIPAC Executive Secretariat. The CIPAC Executive Secretariat will:

A. Attend all CIPAC meetings or designate CISA Federal Compliance Liaison Officials (CLOs) to serve on behalf of the DFO and ensure the advisory activities of CIPAC are within its authorized scope of responsibility, to include exercising the power to adjourn any of its meetings if necessary.

B. Oversee the development, implementation, operation, and observance of compliance procedures and guidelines for CIPAC.

C. Issue guidance for participation in CIPAC and facilitate an annual briefing to provide training to all CIPAC members and participants with respect to such topics as ethics, procurement, and intellectual property as they relate to CIPAC activities.

D. Maintain CIPAC meeting agendas on a publicly accessible website unless exigent circumstances prohibit doing so.

E. Maintain a membership list on the publicly available CIPAC website and publish annual updates in the Federal Register to announce changes in CIPAC membership.

F. Extend invitations, as needed, to attend meetings to federal, state, local, tribal, and territorial officials, and other SMEs, as required by CIPAC activities.

G. Approve any CIPAC compliance procedures and guidelines that are consistent with this Charter. Failure to adhere to the CIPAC Charter, Bylaws, or any CIPAC compliance procedures and guidelines, may result in consequences to the non-compliant sector or sectors, including suspension of CIPAC covered activities or termination of an entity's status as a recognized Sector Coordination Council as defined in the National Infrastructure Protection Plan. It is within the DFO's discretion to take other appropriate administrative actions to ensure CIPAC participants' compliance with this Charter. Failure of CIPAC members and/or participants to adhere to the CIPAC compliance procedures and guidelines, to include the Charter and Bylaws, may result in the denial of those participants from participation in CIPAC activities.

H. Perform other administrative functions as required to ensure CIPAC compliance.

10. Meetings - Estimated Number and Frequency:

CIPAC activities are those member activities that will result in and/or are intended to seek consensus advice and recommendations to the federal government.

As they are independent bodies, meetings consisting solely of members of the SCCs, operating without the specific direction of the federal government, or those consisting solely of members of the GCCs, do not constitute meetings of CIPAC. However, if those meetings are intended to provide consensus advice or recommendations to, and at the request of the federal government, they generally must be held in accordance with CIPAC requirements.

CIPAC meetings will be held as frequently as necessary to address critical infrastructure mission requirements.

Due to the sensitive nature of the material discussed, CIPAC meetings will customarily be closed to the public but may be opened by the DFO or ADFO after consultation with the participating sector coordinating council (SCC), government coordinating council (GCC), and/or cross-sector council leadership.

11. Ethics and Integrity Standards:

All CIPAC participants must annually attend a briefing to receive training provided by CISA on the ethics and integrity standards and information sharing requirements applicable to CIPAC.

12. Duration and Termination:

CIPAC shall function on a continuing basis until the earlier of (A) two years from the date of renewal; or (B) termination by the Secretary; provided however, that CIPAC may continue to exist beyond two years from the date of establishment, upon renewal by the Secretary pursuant to section 871(b) of The Act, 6 U.S.C. § 451(b).

13. Membership Composition and Responsibilities

A. CIPAC will be representative of those critical infrastructure sectors identified in, or established by the Secretary, pursuant to *NSM-22: National Security Memorandum on Critical Infrastructure Security and Resilience* or otherwise designated pursuant to federal law. Additional sectors or subsectors established by the Secretary will be publicly announced. Modal sub-councils, properly recognized within a sector by the respective SRMA, will be considered part of that sector for CIPAC activities, and will work with the CIPAC DFO to ensure CIPAC compliance.

B. CIPAC membership will consist of entities representing: (i) the owner and operator members of a DHS-recognized SCC, including their representative trade associations or equivalent organizations; (ii) governmental entities comprising the members of the GCC for each sector, including their representative organizations; (iii) members of cross-sector councils; and (iv) other federal agencies with responsibility for cyber security and critical infrastructure security and resilience activities. Critical infrastructure owners and operators are those entities that own and invest in physical and cyber infrastructure assets, in the systems and processes to secure them and that are held responsible by the public for their operations and response and recovery when their infrastructures are disrupted.

C. While SCCs are self-organized and self-governed, their composition must be recognized by the respective SRMA with an annual acknowledgement to the DFO that the SCC is a balanced representation of owners, operators and trade or equivalent associations when applicable, reflecting diverse professional and technical expertise and perspectives across the various disciplines of the sector.

CEO or other senior executive level decision makers may participate on behalf of their member representatives in the SCC. The SCC must have the ability to identify and invite SMEs as needed. The SRMA's acknowledgement affirms that the SCC's membership is recognized as being able to achieve the Federal Government's objectives for which the SRMA is responsible.

D. To achieve a level of representation commensurate with the vast and complex critical infrastructure landscape, each SCC must strive to achieve the maximum level of owner and operator participation from its respective sector in CIPAC. Each SCC must seek to determine whether to accept new members based on clearly established membership criteria as described in their respective charter. New member organizations joining an SCC are considered members of CIPAC upon notification to the CIPAC Executive Secretariat. For practical governance purposes, SCCs are encouraged to establish a Sector Executive Committee to manage and coordinate council activities under CIPAC.

E. To fully leverage broad-ranging experience and education, CIPAC must be diverse with regard to professional and technical expertise. The council should also reflect the diversity of the nation's people. SCCs are encouraged to include CIPAC member organizations that can provide diverse viewpoints from across the sector to ensure ample opportunities for collective participation and plurality of opinions. Each member organization should select the appropriate representative(s) to participate in CIPAC activities based on necessary specific subject expertise.

F. CISA and SRMAs work with each SCC and cross-sector council to ensure there are enough individuals representing member organizations who are security clearance holders at the secret and TS/SCI levels, to include the chairs, to support the sharing of and acting on classified information for their sector when necessary.

G. To maintain transparency, each SCC, GCC, and cross-sector council convening under CIPAC shall maintain a current, publicly available membership list and a public charter that: is consistent with current presidential directives and executive orders applicable to cyber and critical infrastructure security and resilience; is approved or otherwise ratified by the respective council within the last five years; and describes, at minimum, criteria for determining a balanced and representational membership. CISA, in consultation with the DFO, may consider any entity with a charter exceeding five years inactive with an ability to convene activities under CIPAC revoked and removed from the public CIPAC website until such time a compliant charter is submitted to the CIPAC Executive Secretariat.

H. SMEs are not CIPAC members and may not participate in the deliberative process or in the development of consensus advice, are precluded from serving in a leadership capacity of an SCC or working group or affiliated sub-working group and are not part of CIPAC itself. SMEs must comply with all applicable provisions of this Charter, to include the ethics and integrity requirements, and information sharing responsibilities

and requirements outlined within the Charter and bylaws.

I. SCCs, GCCs, and cross-sector councils must make annual CIPAC ethics and information sharing training available to their respective members and ensure that all members attend a briefing to complete such training in accordance with compliance procedures and guidelines issued by the DFO.

J. Individuals representing non-federal members of CIPAC serve as representatives of their sectors, not as special government employees as defined in 18 U.S.C. § 202(a). Representatives serve without any compensation for their work.

14. Working Groups and Cross-Sector Working Groups:

CIPAC may meet as a whole or in any combination of working groups or affiliated sub-working groups that is most conducive to effectively conduct its activities including, without limitation, groups encompassing specific sectors to address sector-specific issues and concerns, or a cross-sector group with representation from multiple sectors to address interdependencies and other cross-sector issues. SMEs may participate as part of these working groups or sub-working groups but may not serve in a leadership capacity or deliberations that could result in consensus advice or recommendations. (See the definition of a SME in the CIPAC Bylaws, Article III, Section (1)(i)).

Consistent with one of the tenets of the establishment of CIPAC (i.e., the ability to quickly convene relevant critical infrastructure stakeholders), an SRMA, in consultation with the DFO, may establish or otherwise sponsor an ad-hoc working group as the sole chair and determine the working group's appropriate criteria for membership, and SMEs as needed, to address immediate, urgent, and/or emerging threats or issues.

CIPAC compliant cross-sector working groups that are expected to meet to provide consensus advice and/or recommendations are established in compliance with DFO- issued compliance procedures and guidelines, to include a DFO approved charter. To establish a cross-sector working group, see Article IX in the CIPAC bylaws. The charter must not exceed five years, and must define the purpose, scope, desired outcome(s), expected duration, meeting frequency, and membership criteria, including the selection of SMEs needed to address critical infrastructure and resilience activities that are relevant to multiple sectors.

To meet DHS objectives, CISA, in consultation with the DFO, may charter cross-sector working groups and affiliated sub-working groups as sole sponsor and chair and determine the corresponding membership (derived from CIPAC participants) following the provisions and criteria stated in this Charter and compliance procedures and guidelines issued by the DFO.

15. Recordkeeping:

The DFO will prepare and/or otherwise maintain records of all CIPAC meetings—including working groups, and affiliated sub-working groups or cross-sector working groups—that will, at a minimum, contain the membership present, including each member representative's professional affiliation; a description of matters and materials discussed; and any general actions taken, conclusions reached, or recommendations adopted. The DFO maintains all records of CIPAC, in accordance with General Records Schedule 6.2, or other approved agency records disposition schedule. These records will be available to the public in accordance with the Freedom of Information Act (5 U.S.C. § 552).

Signature (signature of the Secretary)

Alejandro N. Mayorkas
Secretary of Homeland Security

Date: SEPT. 9, 2024