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

I. ESTABLISHMENT AND OFFICIAL DESIGNATION

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), 5 U.S.C. App.

II. OBJECTIVE AND SCOPE OF ACTIVITY

A. CIPAC is aligned with and supports the implementation of the National Infrastructure Protection Plan (NIPP) 2013: *Partnering for Critical Infrastructure Security and Resilience,* and will help to effectuate the interests of the partnership structure set forth in the NIPP 2013, or any subsequently dated issuances thereof, by coordinating federal infrastructure security and resilience programs with the infrastructure security and resilience activities of the private sector and of state, local, tribal, and territorial governments. CIPAC also operates consistent with the critical infrastructure sector construct outlined in Presidential Policy Directive - 21(PPD-21), *Critical Infrastructure Security and Resilience*. Specifically, CIPAC will facilitate 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 to conduct deliberations and form consensus positions to assist the Federal Government in engaging in, among other things:

1. Planning;

2. Coordinating with government and critical infrastructure owner and operator partners;

3. Implementing security and resilience program initiatives;

4. Conducting operational activities related to critical infrastructure security and resilience measures, incident response, and recovery;

5. Reconstituting physical and cyber critical infrastructure assets and systems from both manmade and naturally occurring events; and

6. Sharing threat, vulnerability, risk mitigation, business continuity information, best practices, and lessons learned at the unclassified level and as necessary, the classified level with current clearance holders.

B. As appropriate, CIPAC may develop policy advice and recommendations on 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.

1. Department of Homeland Security (DHS);

2. The Sector-Specific Agency (SSA) for each sector; and

3. Other federal departments and agencies supporting the critical infrastructure security and resilience mission under the NIPP 2013, or any subsequently dated issuances thereof, which have responsibility for establishing and implementing federal policy and managing federal programs.

C. CIPAC, its component working groups, and affiliated sub-working groups, may consult with interested U.S. Government parties, agencies, interagency committees, or groups, as well as with non-governmental groups and individuals, in a manner consistent with this Charter.

D. CIPAC activities shall be conducted pursuant to applicable legal authorities and are subject to all laws, regulations, and policies governing the conduct and operations of the Federal Government.

III. DEFINITIONS

A. For the purpose of this Charter and consistent with the NIPP, these following definitions apply:

1. **CIPAC Participant:** CIPAC participant is a collective term referring to all CIPAC members and individuals representing CIPAC members listed in IV.B of this Charter as well as subject matter experts (SME). A CIPAC participant is subject to all provisions of this Charter.

2. **Cross-Sector Councils**: The Cybersecurity and Infrastructure Security Agency (CISA) recognizes several Cross-Sector Councils that function under CIPAC, as identified in the NIPP 2013 or any subsequently dated issuances thereof, including: Critical Infrastructure Cross-Sector Council; Federal Senior Leadership Council; and State, Local, Tribal and Territorial Government Coordinating Council. CISA may recognize other Cross-Sector Councils under CIPAC to address emerging issues impacting critical infrastructure. These Cross-Sector Councils work to create consensus advice or recommendations to

relevant federal agencies and therefore must comply with all provisions in this Charter and compliance procedures and guidelines issued by the CIPAC Designated Federal Officer (DFO).

3. **Cross-Sector Working Groups**: Cross-sector working groups consist of CIPAC members representing more than one PPD-21 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 of the provisions in this Charter and any compliance procedures and guidelines issued by the DFO. Ad-hoc cross-sector groups that meet to provide consensus advice or recommendations also qualify as cross-sector working groups under this Charter.

4. **Designated Federal Officer**: The DFO or Alternate DFO (ADFO) are CISA 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.

5. **Government Coordinating Councils (GCC):** 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.

6. **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 to collaborate with SSAs and related GCCs to address the entire range of critical infrastructure security and resilience activities and issues for that sector.

7. **Sector Specific Agency (SSA)**: PPD-21 identifies 16 critical infrastructure sectors[1] and their assigned SSAs. As the SSA, that federal agency is responsible for the sector's 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.

[1] While PPD-21 identifies 16 Critical Infrastructure Sectors, it acknowledges that sector structure and designations can evolve: "[t]he Secretary of Homeland Security shall periodically evaluate the need for and approve changes to critical infrastructure sectors and shall consult with the Assistant to the President for Homeland Security and Counterterrorism before changing a critical infrastructure sector or a designated SSA for that sector." *See* Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience*, at pp. 14.

8. **Subject Matter Expert (SME)**: An 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. An 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.

9. **Working Groups**: CIPAC working groups and affiliated sub-working groups, regardless of title, consist of CIPAC members from the participating PPD-21 designated sectors or subsectors, and SMEs, as needed, to address the critical infrastructure needs of the sector. These groups meet on a recurring basis to create consensus advice or recommendations to the relevant federal agencies and therefore must comply with all of the provisions in this Charter 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 this Charter.

IV. MEMBERSHIP AND ORGANIZATION

A. CIPAC will be representative of those critical infrastructure sectors identified in, or established by the Secretary, pursuant to PPD-21: Critical Infrastructure Security and Resilience. Additional sectors or subsectors established by the Secretary will be publicly announced. Modal sub-councils, properly established within a sector, 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 (hereinafter "SCC CIPAC Members"); (ii) governmental entities comprising the members of the GCC for each sector, including their representative organizations (hereinafter "GCC CIPAC Members"); (iii) members of the State, Local, Tribal, and Territorial Government Coordinating Council; and (iv) other federal agencies with responsibility for 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 SSA. The SSA must provide an annual acknowledgement to the DFO that the SCC is an appropriate representation of the sector in order to achieve the Federal Government's objectives.

D. CIPAC activities are those member activities that will result in and/or are intended to seek consensus advice and recommendations. SCCs may choose to conduct some additional activities outside of their advisory relationship with the Federal Government, and in doing so, may choose to form legal entities to facilitate that work, as long as those entities are not-for-profit. In their capacity as advisory bodies to the Federal Government, fees or dues may not be used as criteria for membership.

E. In order to achieve as representational a membership as possible from each sector, as new sectors and/or subsectors and their SCCs are formed – and existing ones mature – critical infrastructure owners and operators or their representative trade associations or equivalent organizations that join SCCs after the date of renewal indicated below shall be considered members of CIPAC upon notification to the CIPAC Executive Secretariat.

F. 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 the Federal Government, they generally must be held in accordance with CIPAC requirements.[2] If CIPAC working groups or affiliated sub-working groups are deliberative and are intended to provide consensus advice, then they shall comply with CIPAC requirements as established in this Charter and any compliance procedures and guidelines established by the DFO.

G. CIPAC may meet as a whole or in any combination of working groups or affiliated sub-working groups that is most conducive to the effective conduct of 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 offer consensus advice or recommendations. See the definition of a SME in III (A)(7).

H. Consistent with one of the tenets of the establishment of CIPAC (i.e., the ability to quickly convene relevant critical infrastructure stakeholders), an SSA - in

[2] GCC-only meetings may not be required to be held under CIPAC, even if they are coming to consensus advice, if the meetings are exclusively between Federal officials and elected officers of state, tribal, and local governments (or their authorized designated employees) solely for the purpose of exchanging views, information, or advice relating to the management or implementation of Federal programs established pursuant to public law that explicitly or inherently share intergovernmental responsibilities or administration. *See* Unfunded Mandates Reform Act of 1995 ("UMRA"), 2 U.S.C. § 1534(b) (exempting certain activities from FACA).

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 membership, and SMEs as needed, to address immediate, urgent, and/or emerging threat or issues.

I. . CIPAC 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. In order to establish a cross-sector working group, the SSA(s) and an SCC or Cross-Sector Council must agree there is a need to establish a cross sector working group and must identify individuals to serve as the co-chair(s) to represent the SSA(s) and an SCC or Cross Sector Council. Cross sector working groups must operate in accordance with a working group charter, and the working group charter 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.

J. 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.

K. In order to maintain transparency, each SCC, GCC, and Cross-Sector Council as defined in the NIPP 2013, or any subsequently dated issuances thereof, convening under CIPAC shall maintain a current, publicly available membership list and a public charter that: is consistent with current PPDs and Executive Orders applicable to 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 representative membership.

L. In order 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 participation from its respective sector in CIPAC and may not impose limits on the size of the SCC's membership. Each SCC must seek to determine whether or not to accept new members based on clearly established membership criteria – as described in their respective charter. For practical governance purposes, SCCs are encouraged to establish a Sector Executive Committee to manage and coordinate council activities under CIPAC.

M. In order to ensure ample opportunities for collective participation and plurality of opinions within CIPAC, SCCs are encouraged to appoint multiple CIPAC representatives from various CIPAC member organizations that can provide diverse viewpoints from across the sector.

N. At the direction of the President of the United States and consistent with federal policy, federally registered lobbyists may not participate as SCC member

representatives in a personal or "individual capacity" at meetings convened under CIPAC. This limitation applies only to covered CIPAC activities, which include decision-making, formulating recommendations, and deliberations leading to consensus advice. Federally registered lobbyists who are SCC member representatives or invited SMEs may participate at meetings convened under CIPAC, when functioning in a "representative capacity," such that they are representing the interests of a non-governmental entity or a recognizable group of persons, including, but not limited to, an industry sector, or state and local governments.[3] Federally registered lobbyists representing SCC members may continue to participate in all other NIPP framework meetings and activities outside CIPAC convened events.

O. SMEs shall be used solely to provide technical or industry specific information for the purposes of informing the recommendations of CIPAC members, in order for members to reach consensus on a particular critical infrastructure issue. 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 in Sections VI and VII, respectively.

P. Individuals representing non-federal CIPAC 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.

Q. DHS Components may use CIPAC membership to address emergent threats or issues regarding critical infrastructure on a less formal basis and shall work in consultation with the DFO to ensure CIPAC compliance.

R. Participation in CIPAC does not provide authorization or permission to use any seal, trademark, or visual identities owned by the Federal Government. The use of any seal, trademarks, or other visual identities associated with the Federal Government requires a written agreement between CIPAC member(s) and the relevant federal agency.

S. SCCs, GCCs, and Cross-Sector Councils have a shared responsibility with CISA to ensure CIPAC participants are compliant with the ethics and integrity standards set forth in this Charter. Additionally, SCCs and Cross-Sector Councils must ensure that potential conflicts of interest are promptly reported by CIPAC participants to a

[3] Presidential Memorandum "Lobbyists on Agency Boards and Commissions" issued on June 18, 2010 directs agencies and departments in the Executive Branch not to appoint or re-appoint federally registered lobbyists to advisory committees and other boards and commissions. Further guidance was finalized by the Office of Management and Budget on August 13, 2014, clarifying the ban applies to persons serving in their individual capacity and does not apply if they specifically appointed to represent the interests of nongovernmental entity, recognizable group of persons or nongovernmental entities (an industry sector, labor unions, environmental groups, etc.), or state governments. See 79 FR 47482.

CIPAC Compliance Liaison Official (CLO) or DFO either verbally or in writing, and that any mitigation measures required by the DFO are implemented. GCCs are expected to be familiar with the ethics and integrity standards and information sharing requirements in this Charter and ensure compliance with them.

T. 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 complete such training in accordance with compliance procedures and guidelines issued by the DFO.

V. MEETINGS AND RESPONSIBILITIES

A. CIPAC meetings will be held as frequently as necessary to address critical infrastructure mission requirements. Meetings will be announced on a publicly accessible website unless exigent circumstances prohibit doing so.

B. 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 SCC, GCC, and/or Cross-Sector Council leadership.

C. CISA will be designated as the CIPAC Executive Secretariat. The Director of CISA shall appoint a DFO and ADFO(s) as part of the CIPAC Executive Secretariat. The CIPAC Executive Secretariat will:

1. Through the appointed DFO or ADFO(s) (i) designate CISA Federal Compliance Liaison Officials (CLOs) to attend all CIPAC meetings and ensure the advisory activities of CIPAC are within its authorized scope of responsibility, exercising the power to adjourn any of its meetings if necessary; (ii) annually train and certify CLOs on their required duties; and (iii) prepare public notices related to meetings.

2. Oversee the development, implementation, operation, and observance of compliance procedures and guidelines for CIPAC. It will also issue guidance for participation in CIPAC and facilitate annual training to members with respect to such topics as ethics, procurement, and intellectual property as they relate to CIPAC activities.

3. Prepare and/or otherwise maintain records of all CIPAC meetings – including working groups and affiliated sub-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. All CIPAC records are subject to any relevant federal laws to include the Freedom of Information Act.

4. Maintain calendars and agendas for CIPAC meetings.

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

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

7. Approve any CIPAC compliance procedures and guidelines that are consistent with this Charter. Failure to adhere to this Charter or any CIPAC compliance procedures and guidelines may result in a recommendation from the DFO to the Director of CISA to revoke a council's corresponding charter and terminate its status as part of CIPAC. It is within the DFO's discretion to take other appropriate administrative actions to ensure CIPAC participants' compliance with this Charter. Failure of CIPAC participants to adhere to the CIPAC compliance procedures and guidelines, to include this Charter, may result in the denial of those participants from participation in CIPAC activities.

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

D. CIPAC Executive Secretariat may accept the offer of another federal agency to host and provide secretariat meeting support for any CIPAC meeting that they are conducting as the SSA. 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.

E. CIPAC members must participate according to this Charter and any compliance procedures and guidelines hereafter adopted.

VI. ETHICS AND INTEGRITY STANDARDS

A. CIPAC participants must attend annual training, provided by CISA, on the ethics and integrity standards and information sharing requirements applicable to CIPAC.

B. Non-federal CIPAC participants must sign a standard acknowledgment of CIPAC ethics and integrity standards, which will be provided by CISA. The acknowledgement shall be renewed on an annual basis as part of the annual training requirement. In exigent or urgent circumstances, the DFO may implement ad hoc procedures to obtain ethics acknowledgments or temporarily postpone this requirement until it can be completed by the participant.

C. CIPAC participants shall not take any action that would result in real or perceived preferential treatment for themselves as individuals, for the organization they represent, or any other person or entity.

D. CIPAC participants shall make known to CIPAC CLO or DFO and shall recuse themselves from CIPAC activity when involvement in such a matter would cause a reasonable person with knowledge of the relevant facts to question the participant's

impartiality. Such matters would include but not be limited to matters involving the interests of a CIPAC participant's immediate family, general partner, and any organization in which they serve as an officer, director, trustee, general partner, or employee.

E. CIPAC participants shall only use CIPAC and CIPAC resources to advance the intended objectives of CIPAC. Use of CIPAC or CIPAC resources for a CIPAC participant's personal benefit or the benefit of any other person or entity is prohibited. This includes but is not limited to:

   1. Actively pursuing or requesting a government contract, grant, other transaction, or any other federal award, funding, or government benefit for themselves or any other person or entity. Active pursuit of government funding includes seeking a competitive advantage or unequal access to competitively useful information about government requirements, procurement strategy, solicitation development, federal funding or resources, procurement sensitive information, or any other information that could provide a competitive advantage. Any such conduct by a CIPAC participant shall be referred by CISA to the appropriate Federal contracting official as a potential organizational conflict of interest and other appropriate official(s).

   2. CIPAC participants shall not use CIPAC or CIPAC resources to support completion of deliverables or provide services in connection with a federal procurement contract, financial assistance agreement, or other transaction that CIPAC participant performs.

VII. INFORMATION SHARING RESPONSIBILITIES AND REQUIREMENTS

A. CIPAC participants shall refrain from using information obtained through their participation in CIPAC for their personal benefit or the benefit of any other person or entity.

B. CIPAC participants may not share information obtained through their participation in CIPAC with the public or media unless expressly authorized by the DFO/ADFO.

C. Information shared under CIPAC may be utilized by the Federal government to further the objectives and intent of CIPAC.

D. CIPAC participants who share information that a Federal law and/or regulation protects from public disclosure and/or that may only be used by the government for limited purposes (*e.g.* Protected Critical Infrastructure Information, Critical Electric Infrastructure Information, cyber threat indicators and defensive measures, or trade secrets) must appropriately mark all such information and comply with any applicable laws and regulations. Information must be properly marked and only shared in accordance with a Federal information protection regime in order to ensure protection from disclosure to the public by the Federal government or that limited use restrictions are followed, where protection is authorized by law.

E. Business advertisements, capability statements, funding proposals and/or funding requests of any type shall not be shared under CIPAC.

F. Absent advance specific and explicit agency approval, Federal employees and contractors participating in CIPAC may not share information related to government budgeting, resourcing, federal funding process, non-public/sensitive information, deliberative information, or other non-public information.

VIII. ESTIMATED COSTS, 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) fulltime federal employees with 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. The estimated annual operating costs are $850,000 plus personnel costs for at least five (5) permanent federal staff members. This annual operating cost estimate incorporates operating expenses and administrative costs, but excludes other potential costs, such as invitational travel.

IX. DURATION

CIPAC shall function on a continuing basis until the earlier of (A) two years from the date of renewal indicated below; or (B) termination by the Secretary; provided however, that CIPAC may continue to exist beyond two years from the date of establishment indicated below upon renewal by the Secretary pursuant to section 871 (b) of The Homeland Security Act of 2002, 6 U.S.C. § 451(b).

Acting Secretary of Homeland Security

Date: November 30, 2020