CRITICAL INFRASTRUCTURE PARTNERSHIP ADVISORY COUNCIL FREQUENTLY ASKED QUESTIONS

What is the Critical Infrastructure Partnership Advisory Council (CIPAC)?

CIPAC is an advisory council chartered by the U.S. Department of Homeland Security (DHS) to directly support the implementation of the *National Infrastructure Protection Plan* (National Plan). Using the sector partnership structure, CIPAC provides a forum that enables members of the recognized government coordinating councils (GCCs), sector coordinating councils (SCCs), and cross-sector councils to discuss joint critical infrastructure planning, coordination, implementation, and operational issues, along with other relevant matters.

As appropriate, members deliberate to achieve consensus on policy, advice, and recommendations on discrete critical infrastructure protection, security, and resilience matters to be presented to DHS, the Sector Risk Management Agency (SRMA) for each sector, and other federal departments and agencies supporting the critical infrastructure security and resilience mission under the National Plan.[1]

CIPAC uses a forum and trusted environment that:

- Facilitates the flow of advice and information concerning critical infrastructure security, resilience and protection.
- Fosters effective information sharing.
- Mitigates the risk of compromising vulnerabilities.
- Promotes necessary communications during emergencies.

What does exempt from the Federal Advisory Committee Act mean for CIPAC?

DHS published a Federal Register Notice on March 24, 2006, announcing the establishment of CIPAC pursuant to "Section 871" of the *Homeland Security Act* and its exemption from the *Federal Advisory Committee Act* (FACA). FACA, Public Law 42-463, defines the requirements and regulations for how a federal advisory committee operates. FACA applies to any committee, council, task force, working/sub-working group, or similar group established by statute or used by a federal agency for the purpose of obtaining deliberative input, advice, or recommendations from the private sector and/or other non-federal government entities. FACA meetings are open to the public and require access to meeting materials and timely notice of each meeting to be published in the *Federal Register*.

However, DHS was granted a FACA exemption for CIPAC. Absent this exemption, CIPAC meetings would be open to the public, automatically disclosing any sensitive information presented in the meeting. With this exemption, CIPAC meetings are customarily closed to the public and not published in the *Federal Register.*

Who are the members of CIPAC?

CIPAC membership is composed of organizations that represent the 16 critical infrastructure sectors identified in the National Plan, with each GCC, SCC, and cross-sector council maintaining its own membership. Each member organization selects the appropriate representative(s) to participate in CIPAC activities.

SCCs are self-formed and self-governed entities serving as the principal private sector entity working with government to coordinate activities in a given critical infrastructure sector. SCC members are critical infrastructure owners and operators and/or relevant trade organizations that are representative of their respective sector. Similarly, GCCs are formed as the government counterpart to each SCC to enable interagency and cross-jurisdictional coordination. Each GCC is co-chaired by a representative from the designated SRMA and DHS. GCC members are federal, state, local, tribal, and territorial governmental entities, including their representative trade organizations with critical infrastructure responsibilities.

[1] Sector Specific Agencies (SSAs) are now referred to as Sector Risk Management Agencies (SRMAs) as published in the National Defense Authorization Act Section 9002.

If I am not a member of a GCC or SCC, are there ways to participate in CIPAC?

Due to the sensitive nature of material discussed, CIPAC meetings are customarily closed to the public. Non-members of a GCC or SCC cannot be members of CIPAC but may attend CIPAC meetings and working groups by invitation of a SRMA, GCC, or SCC as subject matter experts (SMEs) on a standing or ad-hoc basis.

What is the role of subject matter experts within CIPAC?

SMEs play a vital role in CIPAC by providing GCCs and SCCs with their knowledge and expertise regarding critical infrastructure issues. An SME is an individual who is not a member representative of a council under CIPAC, who possesses significant expertise and substantive knowledge (greater than a layperson) in a field or industry and works in the relevant field or industry. An SME's role is to provide GCCs and SCCs with information that informs the councils prior to forming their consensus recommendations to DHS, an SRMA, and/or other relevant federal department and agency.

Because SMEs are not members of a GCC or SCC, there are limitations to their participation in CIPAC. SMEs may not participate in the development of consensus advice to be presented to DHS, an SRMA, and/or other relevant federal department or agency. Per the CIPAC charter, a SME cannot serve in a leadership capacity including serving in a leadership capacity on working groups that are held under CIPAC. This would not preclude an SCC from appointing SME leadership for working groups conducting activities outside of CIPAC. SMEs may provide individual advice directly to DHS or an SRMA, separately from CIPAC activities. SMEs may also provide advice to be used by a working group or committee to inform its views; however, at no time shall an SME participate in development of consensus advice. SMEs are also subject to the ethical rules and practices provided in the "What ethical rules and practices must non-Federal CIPAC participants follow?" section.

SMEs may not use CIPAC to propose or submit unsolicited proposals to the government. An unsolicited proposal is a written proposal for a new or innovative idea submitted for the purpose of obtaining a contract with the government. Unsolicited proposals must comply with "Subpart 15.6" of the *Federal Acquisition Regulation* and be submitted to the appropriate point of contact listed at https://www.dhs.gov/unsolicited-proposals.

What determines the need to conduct meetings as CIPAC?

FACA governs the operations of federal advisory committees and is implicated when the federal government meets with non-federal government entities to seek consensus advice or recommendations at the direction of the federal government. FACA is triggered by factors such as meetings occurring on a regular basis, with the same entities, that are intended to seek consensus advice or recommendations. For CIPAC, only those member activities that will result in and/or are intended to seek consensus advice or recommendations must be conducted as CIPAC. Examples of common CIPAC activities are joint membership meetings of GCCs and SCCs, and cross-sector and sector-specific working groups or sub-working groups comprised of both GCC and SCC members taking some action. Meetings solely for the purpose of providing information or briefings do not constitute advisory activities and therefore are not conducted as CIPAC.

What are the requirements and conditions for a CIPAC meeting?

Proposed agendas for CIPAC meetings are submitted to the Designated Federal Officer (DFO) for validation that the meeting's purpose, objectives, and outcomes are related to seeking consensus with respect to critical infrastructure security, resilience and/or protection. Upon the DFO's signature of a Notice of CIPAC Compliance, a high-level meeting agenda is posted on the publicly accessible website, www.dhs.gov/cipac, unless exigent circumstances prohibit doing so.

A DHS Compliance Liaison Official (CLO) certified by the DFO is assigned and attends all CIPAC meetings to ensure compliance, including confirmation that GCC and SCC member representation is present. The CLO restricts attendance to member representatives and invited SMEs identified on the meeting roster.

Pursuant to the August 13, 2014, guidance issued by the Office of Management and Budget, the 2010 presidential ban on lobbyist participation in CIPAC meetings was lifted. The CIPAC charter signed by the Secretary of Homeland Security on November 30, 2018, allows for the participation of federally registered lobbyists as long as that participation is in a representative capacity.

What ethical rules and practices must non-federal CIPAC participants follow?

Non-federal CIPAC participants (i.e. SCC members and SMEs) are required under the CIPAC charter to refrain from taking any action that would result in a real or perceived preferential treatment for any non-federal entity. Information obtained solely by virtue of participation in CIPAC cannot be used to obtain a government contract, grant, or other federal award. Failure to meet this ethical requirement may serve as the basis for the removal of a participant from CIPAC, their respective SCC and bar them from future participation in CIPAC activities.

CIPAC participants are required to disclose any potential conflicts of interest that may affect their impartiality in offering recommendations. DHS is primarily concerned with an organizational conflict of interest caused by a CIPAC participant that is actively pursuing government contracts, grants, or other federal awards or funding directly related to the subject matter. This type of conflict of interest must be reported directly to the CIPAC DFO.

Other types of conflicts of interests should be disclosed within the CIPAC member organization, which will resolve these conflicts within the organization to the extent possible, such as recusing participants with conflicts from consensus forming activities if necessary. If these are impossible to resolve, the organizations should notify the CIPAC DFO. Absent such notification, it will be assumed that in delivering all consensus advice to the federal government, CIPAC organizations are assuring that such advice was developed following all ethical requirements and that any conflicts have been sufficiently mitigated.

What ethical rules and practices must federal CIPAC participants follow?

Federal employees participating in CIPAC as part of their official duties have separate, mandatory ethical requirements. The conduct of executive branch employees is governed by criminal and civil statutes and any additional requirements as established by their specific agencies. Federal employees should consult their supervisors and, if necessary, their agencies' ethics officials for specific guidance.

Federal employees are limited in their ability to accept any gratuity, gift, favor, or other benefit. Employees should consult with their ethics officials prior to accepting any benefit of a monetary value from a non-governmental entity.

How are DHS intellectual property rights addressed within CIPAC?

CIPAC participants are asked not to seek copyright protection for any written recommendations submitted to DHS through CIPAC. This allows DHS to share any such recommendations without limitations within DHS and the federal government.

Participation in CIPAC does not give CIPAC members the ability to use the DHS seal, trademarks, or any other visual identity, owned or associated with the department. Cobranding, or use of the DHS seal alongside the trademark or visual identity of any non-federal entity requires the approval of the DHS Office of Public Affairs and the execution of a co-branding agreement reviewed by the DHS Office of the General Counsel. Stakeholders should contact the CIPAC Executive Secretariat at CIPAC@CISA.DHS.Gov to begin the process if cobranding is desired.

Similarly, the use of any trademark or visual identity associated with DHS requires the approval of the applicable DHS program office and a licensing agreement reviewed by the DHS Office of the General Counsel. Stakeholders should contact the CIPAC Executive Secretariat to begin the process. Similarly, the use of any trademark, agency seal, or visual identity associated with any other Federal agency requires the review and approval of the applicable decision makers for that respective agency.

What are the guidelines for regulatory discussions within CIPAC meetings?

The CIPAC framework provides a relatively private environment in which sensitive matters can be discussed to achieve consensus on recommendations or policy guidance on discrete issues related to the safety, security, and resiliency of our critical infrastructure.

The *Administrative Procedure Act* (APA), Public Law 79–404, 60 Stat. 237, enacted on June 11, 1946, is the United States federal statute that governs the way in which administrative agencies of the federal government of the United States may propose and establish regulations. APA provides, among other things, that federal rulemaking be transparent.

As CIPAC meetings are generally not open to the public, they are not necessarily the appropriate forum in which to discuss prospective rulemaking issues. However, CIPAC meetings may seek feedback from relevant participants prior to the publication of a new or modified rule in the *Federal Register*.

Is CIPAC a rulemaking body?

Per the CIPAC charter, a CIPAC meeting is not a forum to create federal policy. Rather, it is an opportunity for public and private owner and operator representatives of critical infrastructure to discuss a discrete subject and work together to provide recommendations or consensus policy guidance. Those recommendations or policy guidance are not law. The CIPAC body does not have authority to implement action. Its function is to provide recommendations that are then presented to the federal official of the governing body responsible for that sector or issue. Only federal officials of the relevant agency can decide whether to accept the recommendation and implement a policy as a result.

What is the *Freedom of Information Act* (FOIA) and how is it relevant to CIPAC?

The *Freedom of Information Act of 1974* (FOIA) 5 U.S.C. § 552, provides for disclosure of federal agency records and information to the public, unless that information is exempt from disclosure under statutory language and/or any accompanying regulatory and case law. CIPAC records produced at or for CIPAC meetings are subject to FOIA. However, all or part of those records may be exempt from public disclosure due to the applicability of one or more of the FOIA exemptions.

Although FOIA has somewhat different ramifications for private sector participants than state and local government participants, possible disclosure of either party's information could affect information sharing within CIPAC. Thus, FOIA provides for nine exemptions from public disclosure. The most relevant to CIPAC include:

- Exemption 1: Information that is properly classified in the interest of national security, pursuant to *Executive Order 12958*.
- Exemption 3: Information exempted from release by statute.
- Exemption 4: Trade secrets and commercial or financial information which could harm the competitive posture or business interests of a company.
- Exemption 5: Deliberative process privileged information that is withheld to prevent injury to the quality of agency decision-making.
- Exemption 7(E): Information pertaining to law enforcement techniques that if disclosed could be used to circumvent the law.
- Exemption 7(F): Information that if disclosed could reasonably be used to endanger the life or physical safety of any individual.

Determining when information falls under one of the FOIA exemptions is a multistep process. However, the final determination as to which records will or will not be released rests with the FOIA Office, in accordance with the department's internal review process.

Just as FOIA ensures some degree of federal government transparency, each of the 50 states, plus Washington, D.C., has a similar law that applies to information received by state and local governments. These state laws are generally known as "open records" or "sunshine" laws and, although similar, do not completely mirror FOIA in terms of what information is protected from disclosure. State open records laws range from no explicit protection to full protection of information related to critical infrastructure. Therefore, even if information is exempt from disclosure under FOIA, it could potentially be released to the public if the information is considered a public record of a state and the state does not have any applicable exemptions to its open records law.

Generally, state, local, tribal, and territorial participants in CIPAC should contact their immediate agency's attorney and/or their individual attorney general's office to determine the laws in their jurisdiction.

Additional Resources:

For more information on CIPAC, please refer to the CIPAC website, www.dhs.gov/cipac, or e-mail CIPAC@cisa.dhs.gov