strategy to leverage and coordinate budgets and expenditures across Federal agencies. Furthermore, the TMAC is required to submit an annual report to the FEMA Administrator that contains: (1) A description of the activities of the Council; (2) an evaluation of the status and performance of flood insurance rate maps and mapping activities to revise and update Flood Insurance Rate Maps; and (3) a summary of recommendations made by the Council to the FEMA Administrator.

Agenda: The purpose of this meeting is for the TMAC members to hold a vote to submit the final report to the FEMA Administrator. Any related materials will be posted to the FEMA TMAC site prior to the meeting to provide the public an opportunity to review the materials. The full agenda and related meeting materials will be posted for review by Friday, January 15, 2021, at https://www.fema.gov/flood-maps/guidance-partners/technical-mapping-advisory-council.


Notes:
- A description of the activities of the Council;
- An evaluation of the status and performance of flood insurance rate maps and mapping activities to revise and update Flood Insurance Rate Maps;
- A summary of recommendations made by the Council to the FEMA Administrator.
- The purpose of this meeting is for the TMAC members to hold a vote to submit the final report to the FEMA Administrator.
- Any related materials will be posted to the FEMA TMAC site prior to the meeting to provide the public an opportunity to review the materials.
- The full agenda and related meeting materials will be posted for review by Friday, January 15, 2021, at https://www.fema.gov/flood-maps/guidance-partners/technical-mapping-advisory-council.

DEPARTMENT OF HOMELAND SECURITY
Notice of the Renewal of the Critical Infrastructure Partnership Advisory Council Charter

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), DHS.

ACTION: Notice of availability; renewal of the Critical Infrastructure Partnership Advisory Council Charter.

SUMMARY: On November 30, 2020, the Department renewed the Critical Infrastructure Partnership Advisory Council (CIPAC) Charter. Through this notice, the Department is making the renewed CIPAC Charter publicly available and highlighting updated information and guidelines that have been included in the renewed charter.

FOR FURTHER INFORMATION CONTACT: Ginger K. Norris, 202–441–5885, ginger.norris@cisa.dhs.gov.

SUPPLEMENTARY INFORMATION: DHS established the CIPAC on March 24, 2006.1 The CIPAC has been included in the renewed charter. The renewed CIPAC Charter includes updated information and guidelines concerning: (1) The formation, governance, and responsibilities of councils, working groups, and cross-sector activities; (2) ethics and integrity standards applicable to CIPAC participants; (3) information sharing requirements; and (4) provisions authorizing training on new ethics requirements.


Notes:
- The CIPAC was established consistent with 6 U.S.C. 121 and 6 U.S.C. 451(a). Pursuant to the Cybersecurity and Infrastructure Security Agency Act of 2018, the National Protection and Programs Directorate (NPPD) was re-designated as CISA and facilitates interactions between government officials and representatives of owners and/or operators for each of the critical infrastructure sectors established by Presidential Policy Directive 21 and identified in the current National Infrastructure Protection Plan. Please visit https://www.cisa.gov/critical-infrastructure-partnership-advisory-council for more information on CIPAC, activities supported by CIPAC, CIPAC Membership Roster, and Council information.

On November 30, 2020, the Secretary of Homeland Security, renewed the CIPAC Charter for an additional two years. The renewed CIPAC Charter superseded the CIPAC Charter dated November 30, 2018 and is available on the CIPAC website at https://www.cisa.gov/critical-infrastructure-partnership-advisory-council. The renewed CIPAC Charter includes updated information and guidelines concerning: (1) The formation, governance, and responsibilities of councils, working groups, and cross-sector activities; (2) ethics and integrity standards applicable to CIPAC participants; (3) information sharing requirements; and (4) provisions authorizing training on new ethics requirements.