

collection of information at email address: [FEMA-Information-Collections-Management@fema.dhs.gov](mailto:FEMA-Information-Collections-Management@fema.dhs.gov).

**SUPPLEMENTARY INFORMATION:** The Emergency Management Performance Grants Program (EMPG) helps facilitate a national and regional all-hazards approach to emergency response, including the development of a comprehensive program of planning, training, and exercises that provides a foundation for effective and consistent response to any threatened or actual disaster or emergency, regardless of the cause. Section 662 of the Post-Katrina Emergency Management Reform Act of 2006 (6 U.S.C. 762), as amended, empowers the FEMA Administrator to continue implementation of an Emergency Management Performance Grants Program to make grants to States to assist State, local, and tribal governments in preparing for all hazards, as authorized by the Robert T. Stafford Disaster Relief and Emergency Assistance Act (42 U.S.C. 5121 *et seq.*).

#### Collection of Information

*Title:* FEMA Preparedness Grants: Emergency Management Performance Grant (EMPG).

*Type of Information Collection:* Extension, without change, of a currently approved information collection.

*OMB Number:* 1660-0126.

*FEMA Forms:* None.

*Abstract:* The Emergency Management Performance Grants (EMPG) Program assists State and local governments in enhancing and sustaining all-hazards emergency management capabilities. The EMPG Work Plan narrative must demonstrate how proposed projects address gaps, deficiencies, and capabilities in current programs and the ability to provide enhancements consistent with the purpose of the program and guidance provided by FEMA. FEMA uses the information to provide details, timelines, and milestones on proposed projects.

*Affected Public:* State, Local, Territorial, or Tribal Government.

*Number of Respondents:* 58.

*Number of Responses:* 58.

*Estimated Total Annual Burden Hours:* 174 hours.

*Estimated Cost:* The estimated annual cost to respondents for the hour burden is \$9,008.26. There are no annual costs to respondents operations and maintenance costs for technical services. There is no annual start-up or capital costs. The cost to the Federal Government is \$415,206.

#### Comments

Comments may be submitted as indicated in the **ADDRESSES** caption above. Comments are solicited to (a) evaluate whether the proposed data collection is necessary for the proper performance of the agency, including whether the information shall have practical utility; (b) evaluate the accuracy of the agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (c) enhance the quality, utility, and clarity of the information to be collected; and (d) minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated, electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.*, permitting electronic submission of responses.

Dated: January 23, 2017.

**Richard W. Mattison,**

*Records Management Program Chief, Mission Support, Federal Emergency Management Agency, Department of Homeland Security.*

[FR Doc. 2017-02166 Filed 2-1-17; 8:45 am]

**BILLING CODE 9111-46-P**

#### DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2016-0092]

#### The Critical Infrastructure Partnership Advisory Council

**AGENCY:** National Protection and Programs Directorate, DHS.

**ACTION:** Notice of renewal of the Critical Infrastructure Partnership Advisory Council (CIPAC) Charter.

**SUMMARY:** The Department of Homeland Security (DHS) announced the establishment of the CIPAC in a **Federal Register** Notice (71 FR 14930-14933) dated March 24, 2006, which identified the purpose of CIPAC, as well as its membership. This notice provides: (i) Notification of the CIPAC charter renewal.

**FOR FURTHER INFORMATION CONTACT:** Renee Murphy, Designated Federal Officer, Critical Infrastructure Partnership Advisory Council, Sector Outreach and Programs Division, Office of Infrastructure Protection, National Protection and Programs Directorate, U.S. Department of Homeland Security, 245 Murray Lane, Mail Stop 0607, Arlington, VA 20598-0607; telephone: (703) 603-5083; email: [CIPAC@hq.dhs.gov](mailto:CIPAC@hq.dhs.gov).

*Responsible DHS Official:* Renee Murphy, Designated Federal Officer for the CIPAC.

#### SUPPLEMENTARY INFORMATION:

*Notice of CIPAC Charter Renewal:* The CIPAC Charter was signed by Secretary of Homeland Security Jeh Johnson on November 30, 2016. It supersedes the CIPAC Charter dated December 7, 2014 and is available on the CIPAC Web site (<http://www.dhs.gov/cipac>).

*Purpose and Activity:* The CIPAC facilitates interaction between government officials and representatives of the community of owners and/or operators for each of the critical infrastructure sectors defined by Presidential Policy Directive 21 and identified in *National Infrastructure Protection Plan 2013: Partnering for Critical Infrastructure Security and Resilience* (NIPP 2013). The scope of activities covered by the CIPAC includes: Planning; coordinating among government and critical infrastructure owner and operator security partners; implementing security program initiatives; conducting operational activities related to critical infrastructure protection security measures, incident response, recovery, and infrastructure resilience; reconstituting critical infrastructure assets and systems for both manmade and naturally occurring events; and sharing threat, vulnerability, risk mitigation, and infrastructure continuity information.

*Organizational Structure:* CIPAC members are organized into 16 critical infrastructure sectors. These sectors have a Government Coordinating Council (GCC) whose membership includes: (i) A lead Federal agency that is defined as the Sector-Specific Agency (SSA); (ii) all relevant Federal, State, local, tribal, and/or territorial government agencies (or their representative bodies) whose mission interests also involve the scope of the CIPAC activities for that particular sector; and (iii) a Sector Coordinating Council (SCC), where applicable, whose membership includes critical infrastructure owners and/or operators or their representative trade associations.

*CIPAC Membership:* CIPAC Membership may include:

(i) Critical Infrastructure owner and operator members of a DHS-recognized SCC, including their representative trade associations or equivalent organization members of a SCC as determined by the SCC.

(ii) Federal, State, local, and tribal governmental entities comprising the

members of the GCC for each sector, including their representative organizations; members of the State, Local, Tribal, and Territorial Government Coordinating Council; and representatives of other Federal agencies with responsibility for Critical Infrastructure activities.

*CIPAC Membership Roster and Council Information:* CIPAC membership is organizational. Multiple individuals may participate in CIPAC activities on behalf of a member organization. Members of the public may visit the CIPAC Web site (<http://www.dhs.gov/cipac>) at any time to view current CIPAC membership, as well as the current and historic lists of CIPAC meetings and agendas.

Dated: January 23, 2017.

**Renee Murphy,**

*Designated Federal Officer for the CIPAC.*

[FR Doc. 2017-02167 Filed 2-1-17; 8:45 am]

**BILLING CODE 9110-9P-P**

## DEPARTMENT OF HOMELAND SECURITY

### Office of the Secretary

[Docket No. DHS-2017-0009]

### DHS Data Privacy and Integrity Advisory Committee

**AGENCY:** Privacy Office, DHS.

**ACTION:** Committee Management; Notice of Federal advisory committee meeting.

**SUMMARY:** The DHS Data Privacy and Integrity Advisory Committee will conduct a teleconference on Tuesday, February 21, 2017. The teleconference will be open to the public.

**DATES:** The DHS Data Privacy and Integrity Advisory Committee will conduct a teleconference on Tuesday, February 21, 2017, from 10:00 a.m. to 12:00 p.m. Please note that the teleconference may end early if the Committee has completed its business.

**ADDRESSES:** This will be a call and online forum (URL will be posted on the Privacy Office Web site in advance of the meeting at [www.dhs.gov/privacy-advisory-committees](http://www.dhs.gov/privacy-advisory-committees)). For information on services for individuals with disabilities, or to request special assistance, contact Sandra Taylor, Designated Federal Officer, DHS Data Privacy and Integrity Advisory Committee, as soon as possible.

To facilitate public participation, we invite public comment on the issues to be considered by the Committee as listed in the **SUPPLEMENTARY INFORMATION** section below. A public comment period will be held during the

meeting from 11:45 a.m.–12:00 p.m., and speakers are requested to limit their comments to three minutes. If you would like to address the Committee at the meeting, we request that you register in advance. The names and affiliations, if any, of individuals who address the Committee are included in the public record of the meeting. Please note that the public comment period may end before the time indicated, following the last call for comments. Written comments should be sent to Sandra Taylor, Designated Federal Officer, DHS Data Privacy and Integrity Advisory Committee, by February 13, 2017. Persons who wish to submit comments and who are not able to attend or speak at the meeting may submit comments at any time. All submissions must include the Docket Number (DHS-2017-0009) and may be submitted by any one of the following methods:

- *Federal eRulemaking Portal:* <http://www.regulations.gov>. Follow the instructions for submitting comments.

- *E-mail:* [PrivacyCommittee@hq.dhs.gov](mailto:PrivacyCommittee@hq.dhs.gov). Include the Docket Number (DHS-2017-0009) in the subject line of the message.

- *Fax:* (202) 343-4010.

- *Mail:* Sandra Taylor, Designated Federal Officer, Data Privacy and Integrity Advisory Committee, Department of Homeland Security, 245 Murray Lane SW., Mail Stop 0655, Washington, DC 20528.

*Instructions:* All submissions must include the words “Department of Homeland Security Data Privacy and Integrity Advisory Committee” and the Docket Number (DHS-2017-0009). Comments received will be posted without alteration at <http://www.regulations.gov>, including any personal information provided.

The DHS Privacy Office encourages you to register for the meeting in advance by contacting Sandra Taylor, Designated Federal Officer, DHS Data Privacy and Integrity Advisory Committee, at [PrivacyCommittee@hq.dhs.gov](mailto:PrivacyCommittee@hq.dhs.gov). Advance registration is voluntary. The Privacy Act Statement below explains how DHS uses the registration information you may provide and how you may access or correct information retained by DHS, if any.

*Docket:* For access to the docket to read background documents or comments received by the DHS Data Privacy and Integrity Advisory Committee, go to <http://www.regulations.gov> and search for docket number DHS-2017-0009.

**FOR FURTHER INFORMATION CONTACT:** Sandra Taylor, Designated Federal

Officer, DHS Data Privacy and Integrity Advisory Committee, Department of Homeland Security, 245 Murray Lane SW., Mail Stop 0655, Washington, DC 20528, by telephone (202) 343-1717, by fax (202) 343-4010, or by email to [PrivacyCommittee@hq.dhs.gov](mailto:PrivacyCommittee@hq.dhs.gov).

**SUPPLEMENTARY INFORMATION:** Notice of this meeting is given under the Federal Advisory Committee Act (FACA), Title 5, U.S.C., appendix. The DHS Data Privacy and Integrity Advisory Committee provides advice at the request of the Secretary of Homeland Security and the DHS Chief Privacy Officer on programmatic, policy, operational, administrative, and technological issues within DHS that relate to personally identifiable information, as well as data integrity and other privacy-related matters. The Committee was established by the Secretary of Homeland Security under the authority of 6 U.S.C. 451.

### Proposed Agenda

During the teleconference, the Committee will address and vote on draft recommendations for DHS to consider on best practices for a data breach notification should DHS suffer a significant incident. The final agenda will be posted on or before January 30, 2017, on the Committee’s Web site at [www.dhs.gov/privacy-advisory-committees](http://www.dhs.gov/privacy-advisory-committees). Please note that the call may end early if all business is completed.

### Privacy Act Statement: DHS’s Use of Your Information

*Authority:* DHS requests that you voluntarily submit this information under its following authorities: The *Federal Records Act*, 44 U.S.C. 3101; the *FACA*, 5 U.S.C. appendix; and the *Privacy Act of 1974*, 5 U.S.C. 552a.

*Principal Purposes:* When you register to attend a DHS Data Privacy and Integrity Advisory Committee meeting, DHS collects your name, contact information, and the organization you represent, if any. We use this information to contact you for purposes related to the meeting, such as to confirm your registration, to advise you of any changes in the meeting, or to assure that we have sufficient materials to distribute to all attendees. We may also use the information you provide for public record purposes such as posting publicly available transcripts and meeting minutes.

*Routine Uses and Sharing:* In general, DHS will not use the information you provide for any purpose other than the Principal Purposes, and will not share this information within or outside the agency. In certain circumstances, DHS