other forms of information technology. Consideration will be given to comments and suggestions submitted within 60 days of this publication.

Robert Sargis,

Reports Clearance Officer.

[FR Doc. 2013–22774 Filed 9–18–13; 8:45 am]

BILLING CODE 4184–01–P

DEPARTMENT OF HOMELAND SECURITY

Agency Information Collection Activities: Department of Homeland Security (DHS) Cybersecurity Education Office (CEO) National Initiative for Cybersecurity Careers and Studies (NICCS) Cybersecurity Training and Education Catalog (Training Catalog) Collection

AGENCY: Cybersecurity Education Office, DHS.

ACTION: 30-Day Notice and request for comments; New Collection (Request for a new OMB Control No.), 1601–NEW.

SUMMARY: The Department of Homeland Security, Cybersecurity Education Office, DHS will submit the following information collection request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995 (Pub. L. 104–13, 44 U.S.C. Chapter 35). DHS previously published this information collection request (ICR) in the **Federal Register** on June 12, 2013 at 78 FR 35295, for a 60-day public comment period. No comments were received by DHS. The purpose of this notice is to allow additional 30-days for public comments.

DATES: Comments are encouraged and will be accepted until October 21, 2013. This process is conducted in accordance with 5 CFR 1320.10.

ADDRESSES: Interested persons are invited to submit written comments on the proposed information collection to the Office of Information and Regulatory Affairs, Office of Management and Budget. Comments should be addressed to OMB Desk Officer, Department of Homeland Security and sent via electronic mail to *oira_submission@omb.eop.gov* or faxed to (202) 395–5806.

The Office of Management and Budget is particularly interested in comments which:

1. Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility;

2. 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;

3. Enhance the quality, utility, and clarity of the information to be collected; and

4. 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 submissions of responses.

FOR FURTHER INFORMATION CONTACT: If additional information is required contact: The Department of Homeland Security (DHS), Cybersecurity Education Office, DHS Attn.: Michael Wigal, *dhs.pra@hq.dhs.gov.*

SUPPLEMENTARY INFORMATION: Title II, Homeland Security Act, 6 U.S.C. 121(d)(1) To access, receive, and analyze law enforcement information, intelligence information and other information from agencies of the Federal Government, State and local government agencies * * * and Private sector entities and to integrate such information in support of the mission responsibilities of the Department. The following authorities also permit DHS to collect information of the type contemplated: Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. 3546; Homeland Security Presidential Directive (HSPD) 7, ''Critical Infrastructure Identification, Prioritization, and Protection'' (2003); and NSPD–54/HSPD–23, ''Cybersecurity Policy'' (2009).

In May 2009, the President ordered a Cyberspace Policy Review to develop a comprehensive approach to secure and defend America's infrastructure. The review built upon the Comprehensive National Cybersecurity Initiative (CNCI).

In response to increased cyber threats across the Nation, the National Initiative for Cybersecurity Education (NICE) expanded from a previous effort, the CNCI #8. NICE formed in March 2011, and is a nationally coordinated effort comprised of over 20 federal departments and agencies, and numerous partners in academia and industry. NICE focuses on cybersecurity awareness, education, training and professional development. NICE seeks to encourage and build cybersecurity awareness and competency across the Nation and to develop an agile, highly skilled cybersecurity workforce.

The NICCS Portal is a national online resource for cybersecurity awareness, education, talent management, and professional development and training. NICCS Portal is an implementation tool for NICE. Its mission is to provide comprehensive cybersecurity resources to the public.

To promote cybersecurity education, and to provide a comprehensive resource for the Nation, NICE developed the Cybersecurity Training and Education Catalog. The Cybersecurity Training and Education Catalog will be hosted on the NICCS Portal. Both Training Course and Certification information will be stored in the Training Catalog.

Note: Any information received from the public in support of the NICCS Portal and Cybersecurity Training and Education Catalog is completely voluntary. Organizations and individuals who do not provide information can still utilize the NICCS Portal and Cybersecurity Training and Education Catalog without restriction or penalty. An organization or individual who wants their information removed from the NICCS Portal and/or Cybersecurity Training and Education Catalog can email the NICCS Supervisory Office (SO).

Department of Homeland Security (DHS) Cybersecurity Education Office (CEO) intends for the collected information from the NICCS Cybersecurity Training Course Form and the NICCS Cybersecurity Certification Form to be displayed on a publicly accessible Web site called the National Initiative for Cybersecurity Careers and Studies (NICCS) Portal (*http://niccs.us-cert.gov/*). Collected information from the NICCS Cybersecurity Training Course Form and the NICCS Cybersecurity Certification Form will be included in the Cybersecurity Training and Education Catalog. Both sets of information will be made available to the public to support the National Initiative for Cybersecurity Education (NICE) mission and the Comprehensive National Cybersecurity Initiative (CNCI)—Initiative 8: Expand Cyber Education.

The DHS CEO NICCS Supervisory Office will use information collected from the NICCS Vetting Criteria Form to primarily manage communications with the training providers; this collected information will not be shared with the public and is intended for internal use only. Additionally, this information will be used to validate training providers and certification owners before uploading their training course or certification information to the Training Catalog.

The information will be completely collected via electronic means. Collection will be exchanged between the public and DHS CEO via email (*niccs@hq.dhs.gov*). All information collected from the NICCS Cybersecurity Training Course Form and the follow-on NICCS Cybersecurity Training Course Web Form will be stored in the publicly accessible NICCS Cybersecurity Training and Education Catalog (*http://nics.us-cert.gov/training/training-home*). The NICCS Cybersecurity Certification Form and follow-on NICCS Cybersecurity Certification Web Form will also be stored in the publicly accessible NICCS Cybersecurity Training and Education Catalog (*http://nics.us-cert.gov/training/training-home*).

The NICCS SO will electronically store information collected via the NICCS Vetting Criteria Form. This information will not be publicly accessible

Analysis

Agency: Cybersecurity Education Office, DHS.

Title: Department of Homeland Security (DHS) Cybersecurity Education Office (CEO) National Initiative for Cybersecurity Careers and Studies (NICCS) Cybersecurity Training and Education Catalog (Training Catalog) Collection

OMB Number: 1601–NEW.

Number of Respondents: 300.

Estimated Number of Responses: 2100.

Estimated Time per Respondent: 1 hour.

Total Burden Hours: 2100 hours.

Dated: September 5, 2013.

Margaret H. Graves,

Acting Chief Information Officer.

[FR Doc. 2013–22831 Filed 9–18–13; 8:45 am]

BILLING CODE 4410–9B–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2103–0050]

Critical Infrastructure Partnership Advisory Council (CIPAC)

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Committee management; Notice of an open Federal Advisory Committee Meeting.

SUMMARY: The Critical Infrastructure Partnership Advisory Council (CIPAC) Plenary Meeting will be held on Tuesday, November 5, 2013, at the Washington DC Convention Center located at 801 Mount Vernon Place NW., Washington, DC 20001. The meeting will be open to the public.

DATES: The CIPAC Plenary will be held on Tuesday, November 5, 2013, from 8:30 a.m. to 4:00 p.m. Registration will begin at 7:30 a.m. For additional information, please consult the CIPAC Web site, *http://www.dhs.gov/cipac,* or contact the CIPAC Secretariat by phone at (703)235–3999 or by email at *CIPAC@hq.dhs.gov.*

ADDRESSES: The meeting will be held at the Washington DC Convention Center, 801 Mount Vernon Place, Washington, DC 20001.

While this meeting is open to the public, participation in the CIPAC deliberations is limited to committee members, Department of Homeland Security officials and persons invited to attend the meeting for special presentations. Immediately following the committee member deliberation and discussion period, there will be a limited time period for public comment. This public comment period is designed for substantive commentary that must pertain only to matters involving critical infrastructure security and resiliency. Off-topic questions or comments will not be permitted or discussed. Please note that the public comment period may begin prior to 3:00 p.m. if the committee has completed its business. To accommodate as many speakers as possible, oral presentations will be limited to three (3) minutes per speaker, with no more than 30 minutes for all speakers. Parties interested in presenting must register in person at the meeting location. Oral presentations will be permitted on a first-come, first-serve basis, and given based upon the order of registration; all registrants may not be able to speak if time does not permit.

Written comments are welcome at any time prior to or following the meeting. Written comments may be sent to Renee Murphy, Department of Homeland Security, National Protection and Programs Directorate, 245 Murray Lane SW., Mail Stop 0607, Arlington, VA 20598–0607. For consideration in the CIPAC deliberations, written comments must be received by Renee Murphy by no later than 12:00 p.m. on September 24, 2013, identified by **Federal Register** Docket Number DHS–2013–0050 and may be submitted by one of the following methods:

- *Federal eRulemaking Portal: www.regulations.gov.* Follow the instructions for submitting written comments.
- *Email: CIPAC@hq.dhs.gov.* Include the docket number in the subject line of the message.
- *Fax:* (703)603–5098.
- *Mail:* Renee Murphy, National Protection and Programs Directorate, Department of Homeland Security, 245 Murray Lane SW., Mail Stop 0607, Arlington, VA 20598–0607.

Instructions: All written submissions received must include the words ''Department of Homeland Security'' and the docket number for this action. Written comments received will be posted without alteration at *http://www.regulations.gov,* including any personal information provided.

Docket: For access to the docket to read background documents or comments received by the CIPAC, go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION, CONTACT: Renee Murphy, Critical Infrastructure Partnership Advisory Council Alternate Designated Federal Officer, telephone (703) 235–3999.

SUPPLEMENTARY INFORMATION: CIPAC represents a partnership between the Federal Government and critical infrastructure owners and operators, and provides a forum in which they can engage in a broad spectrum of activities to support and coordinate critical infrastructure security and resilience. The September 25, 2013, meeting will include topic-specific discussions focused on partnership efforts to enhance critical infrastructure resilience. Topics such as the Executive Order for Improving Critical Infrastructure Cybersecurity, Presidential Policy Directive 21—Critical Infrastructure Security and Resilience, and Critical Infrastructure Program Updates will be discussed.

Information on Services for Individuals With Disabilities: For information on facilities or services for individuals with disabilities or to request special assistance at the meeting, contact the CIPAC Secretariat at (703) 235–3999 as soon as possible.

Dated: September 12, 2013.

Larry May,

Designated Federal Officer for the CIPAC.

[FR Doc. 2013–22830 Filed 9–18–13; 8:45 am]

BILLING CODE 4410–9P–P