improve IP's CIKR prioritization efforts; this list is called the Critical Infrastructure List.

The Critical Infrastructure List includes assets and systems that, if destroyed, damaged or otherwise compromised, could result in significant consequences on a regional or national scale. This list provides a common basis for DHS and its security partners during the undertaking of CIKR protective planning efforts to keep our Nation safe. Collection of this information is directed and supported by Public Law 110–53 ''Implementing Recommendations of the 9/11 Commission Act of 2007,'' August 3, 2007; and Homeland Security Presidential Directive (HSPD) 7, ''Critical Infrastructure Identification, Prioritization, and Protection,'' December 17, 2003.

Dated: September 25, 2008.

Chase Garwood,

Chief Information Officer, National Protection and Programs Directorate, Department of Homeland Security.

Editorial Note: This document was received in the Office of the Federal Register on Thursday, January 8, 2009.

[FR Doc. E9–567 Filed 1–13–09; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

National Protection and Programs Directorate; Submission for Review: Critical Infrastructure and Key Resources Asset Protection Technical Assistance Program (CAPTAP) Train the Trainer Survey 1670—NEW

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

ACTION: 30-Day Notice and request for comments.

SUMMARY: The Department of Homeland Security (DHS) invites the general public and other federal agencies to comment on new information collection request 1670—NEW, CAPTAP Train the Trainer Survey. As required by the Paperwork Reduction Act of 1995, (Pub. L. 104–13, 44 U.S.C. chapter 35) as amended by the Clinger-Cohen Act (Pub. L. 104–106), DHS is soliciting comments for this collection. The information collection was previously published in the **Federal Register** on August 1, 2008 at 73 FR 45025 allowing for a 60-day public comment period. No comments were received on this existing information collection. The purpose of this notice is to allow an additional 30 days for public comments.

DATES: Comments are encouraged and will be accepted until February 13, 2009. This process is conducted in accordance with 5 CFR 1320.1.

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, 725 17th Street, NW., Washington, DC 20503, Attention: Desk Officer for National Protection and Programs Directorate, DHS or sent via electronic mail to *oira_submission@omb.eop.gov* or faxed to (202) 395–6974.

FOR FURTHER INFORMATION CONTACT: A copy of this ICR, with applicable supporting documentation, may be obtained by contacting the Office of Information and Regulatory Affairs, Office of Management and Budget, 725 17th Street, NW., Washington, DC 20503, Attention: Desk Officer for National Protection and Programs Directorate, DHS or via electronic mail to *oira_submission@omb.eop.gov*.

SUPPLEMENTARY INFORMATION: The Office of Management and Budget is particularly interested in comments that:

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.

Analysis

Agency: Department of Homeland Security, National Protection and Programs Directorate, Infrastructure Protection.

Title: CAPTAP Train the Trainer Survey.

OMB Number: 1670—NEW.

Frequency: Once.

Affected Public: State, Local, Tribal.

Number of Respondents: 150.

Estimated Time per Respondent: 12 minutes.

Total Burden Hours: 30 hours.

Total Burden Cost (capital/startup): None.

Total Burden Cost (operating/maintaining): None.

Description: The C/ACAMS program uses the CAPTAP Train the Trainer survey to assess participant satisfaction with the training. The survey supports decision-making by identifying actionable training data to reallocate resources to address it. The Train the Trainer survey collects data about participants' satisfaction with the instructors, materials, course curriculum, activities and applicability to effect cost savings by prioritizing training improvements.

Dated: November 6, 2008.

Chase Garwood,

Chief Information Officer, National Protection and Programs Directorate Department of Homeland Security.

[FR Doc. E9–570 Filed 1–13–09; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2008–0196]

Homeland Security Science and Technology Advisory Committee

AGENCY: Science and Technology Directorate, DHS.

ACTION: Committee Management; Notice of Closed Federal Advisory Committee Meeting.

SUMMARY: The Homeland Security Science and Technology Advisory Committee will meet January 26–28, 2009 at Johns Hopkins University/Applied Physics Laboratory in Laurel, MD. The meeting will be closed to the public.

DATES: The Homeland Security Science and Technology Advisory Committee will meet January 26, 2009, from 2 p.m. to 4:30 p.m., January 27, 2009, from 8:30 a.m. to 4:30 p.m. and on January 28, 2009, from 8 a.m. to 12 p.m.

ADDRESSES: The meeting will be held at Johns Hopkins University/Applied Physics Laboratory, 11100 Johns Hopkins Road, Laurel, MD. Requests to have written material distributed to each member of the committee prior to the meeting should reach the contact person at the address below by Friday, January 16, 2009. Send written material to Ms. Deborah Russell, Science and Technology Directorate, Department of Homeland Security, 245 Murray Lane, Bldg. 410, Washington, DC 20528. Comments must be identified by DHS–

2008–0196 and may be submitted by one of the following methods:

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

• *E-mail: HSSTAC@dhs.gov.* Include the docket number in the subject line of the message.

• *Fax:* 202–254–6173.

• *Mail:* Ms. Deborah Russell, Science and Technology Directorate, Department of Homeland Security, 245 Murray Lane, Bldg. 410, Washington, DC 20528.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and the docket number for this action. 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 Homeland Security Science and Technology Advisory Committee, go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Ms. Deborah Russell, Science and Technology Directorate, Department of Homeland Security, 245 Murray Lane, Bldg. 410, Washington, DC 20528 202–254–5739.

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the Federal Advisory Committee Act, 5 U.S.C. App. (Pub. L. 92–463).

The committee will meet for the purpose of receiving classified and sensitive Homeland Security and classified briefings on Maritime Improvised Explosive Devices (IEDs), Cyber Security and Science and Technology Programs.

Basis for Closure: In accordance with Section 10(d) of the Federal Advisory Committee Act, it has been determined that the Science and Technology Advisory Committee meeting concerns sensitive Homeland Security information and classified matters within the meaning of 5 U.S.C. 552b(c)(1) and (c)(9)(B) which, if prematurely disclosed, would significantly jeopardize national security and frustrate implementation of proposed agency actions.

Dated: January 6, 2009.

Jay M. Cohen,

Under Secretary for Science and Technology.

[FR Doc. E9–569 Filed 1–13–09; 8:45 am]

BILLING CODE 4410–10–P

DEPARTMENT OF HOMELAND SECURITY

National Communications System

[Docket No. NCS–2008–0004]

President's National Security Telecommunications Advisory Committee

AGENCY: National Communications System, DHS.

ACTION: Notice of Partially Closed Advisory Committee Meeting.

SUMMARY: The President's National Security Telecommunications Advisory Committee (NSTAC) will be meeting by teleconference; the meeting will be partially closed to the public.

DATES: February 10, 2009, from 2 p.m. until 3 p.m.

ADDRESSES: The meeting will take place by teleconference. For access to the conference bridge and meeting materials, contact Ms. Sue Daage at (703) 235–5526 or by e-mail at *sue.daage@dhs.gov* by 5 p.m. February 1, 2009. If you desire to submit comments regarding the February 10, 2009, meeting they must be submitted by February 17, 2009. Comments must be identified by NCS–2008–0004 and may be submitted by one of the following methods:

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

E-mail: NSTAC1@dhs.gov. Include docket number in the subject line of the message.

Mail: Office of the Manager, National Communications System (Customer Service Branch), Department of Homeland Security, 1100 Hampton Park Blvd., Capitol Heights, MD 20743;

Fax: 1–866–466–5370.

Instructions: All submissions received must include the words ''Department of Homeland Security'' and NCS–2008–0004, the docket number for this action. 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 NSTAC, go to *http://www.regulations.gov.*

FOR FURTHER INFORMATION CONTACT: Ms. Sue Daage, Customer Service Branch at (703) 235–5526, e-mail: *sue.daage@dhs.gov* or write the Deputy Manager, National Communications System, Department of Homeland Security, 1100 Hampton Park Blvd., Capitol Heights, MD 20743.

SUPPLEMENTARY INFORMATION: NSTAC advises the President on issues and problems related to implementing national security and emergency preparedness telecommunications policy. Notice of this meeting is given under the Federal Advisory Committee Act (FACA), Public Law 92–463 (1972), as amended appearing in 5 U.S.C. App. 2.

At the upcoming meeting, between 2 p.m. and 2:15 p.m., the conference call will include government stakeholder feedback on NSTAC initiatives, and a status report on NSTAC Recommendations. This portion of the meeting will be open to the public.

Between 2:15 p.m. and 3 p.m., the NSTAC will discuss and vote on the Global Resiliency Report and receive three updates from the identity management, cybersecurity and satellite network task forces. This portion of the meeting will be closed to the public.

Persons with disabilities who require special assistance should indicate this when arranging access to the teleconference and are encouraged to identify anticipated special needs as early as possible.

Basis for Closure: During the portion of the meeting to be held from 2:15 p.m. to 3 p.m., the NSTAC will discuss core assurance and physical security of the cyber network, cybersecurity collaboration between the Federal government and the private sector, identity management issues and cyber-related vulnerabilities of the satellite network. Such discussions will likely include internal agency personnel rules and practices, specifically, identification of vulnerabilities in the Federal government's cyber network, along with strategies for mitigating those vulnerabilities and other sensitive law enforcement or homeland security information of a predominantly internal nature which, if disclosed, would significantly risk circumvention of DHS regulations or statutes. NSTAC members will likely inform the discussion by contributing confidential and voluntarily-provided commercial information relating to private sector network vulnerabilities that they would not customarily release to the public. Disclosure of this information can be reasonably expected to frustrate DHS's ongoing cybersecurity programs and initiatives and could be used to exploit vulnerabilities in the Federal government's cyber network. Accordingly, the relevant portion of this meeting will be closed to the public