the authority for ICCVAM involvement in activities relevant to the development of alternative test methods. ICCVAM acts to ensure that new and revised test methods are validated to meet the needs of Federal agencies, increase the efficiency and effectiveness and Federal agency test method review, and optimize utilization of scientific expertise outside the Federal Government. Additional information about ICCVAM can be found at *http://ntp.niehs.nih.gov/go/iccvam*.

NICEATM administers ICCVAM, provides scientific and operational support for ICCVAM-related activities, and conducts independent validation studies to assess the usefulness and limitations of new, revised, and alternative test methods and strategies. NICEATM and ICCVAM work collaboratively to evaluate new and improved test methods and strategies applicable to the needs of U.S. Federal agencies. NICEATM and ICCVAM welcome the public nomination of new, revised, and alternative test methods and strategies for validation studies and technical evaluations. Additional information about NICEATM can be found at *http://ntp.niehs.nih.gov/go/niceatm*.

Dated: April 24, 2014.

John R. Bucher,

Associate Director, National Toxicology Program.

[FR Doc. 2014–10015 Filed 5–1–14; 8:45 am]

BILLING CODE 4140–01–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2013–0067]

Sector Outreach and Programs Division Online Meeting Registration Tool

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: 30-day notice and request for comments; Renewal Information Collection Request: 1670–0019.

SUMMARY: The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office Of Infrastructure Protection (IP), Sector Outreach and Programs Division (SOPD), will submit the following Information Collection Request 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). NPPD is soliciting comments concerning Renewal Information Collection Request, Sector Outreach and Programs Division Online Meeting Registration Tool. DHS previously published this ICR in the **Federal Register** on February 10, 2014, for a 60-day public comment period. DHS received no comments. The purpose of this notice is to allow an additional 30 days for public comments.

DATES: Comments are encouraged and will be accepted until June 2, 2014. 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, OMB. Comments should be addressed to OMB Desk Officer, Department of Homeland Security, Office of Civil Rights and Civil Liberties. Comments must be identified by DHS–2013–0067 and may be submitted by one of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov*.
- *Email: oira_submission@omb.eop.gov*. Include the docket number in the subject line of the message.
- *Fax:* (202) 395–5806

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.

OMB 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.

FOR FURTHER INFORMATION CONTACT: Nohemi Zerbi DHS/NPPD/IP/SOPD/COG, *Nohemi.Zerbi@hq.dhs.gov*.

SUPPLEMENTARY INFORMATION: On behalf of DHS, IP manages the Department's program to protect the Nation's 16 Critical Infrastructure and Key Resource (CIKR) Sectors by implementing the National Infrastructure Protection Plan (NIPP) 2013 Partnering for Critical Infrastructure Security and Resilience . Pursuant to Presidential Policy Directive (PPD)—21 (February 2013), each sector is assigned a Sector Specific Agency (SSA) to oversee Federal interaction with the array of sector security partners, both public and private. An SSA is responsible for leading a unified public-private sector effort to develop, coordinate, and implement a comprehensive physical, human, and cybersecurity strategy for its assigned sector. SOPD executes the SSA responsibilities for the six CIKR sectors assigned to IP: Chemical; Commercial Facilities; Critical Manufacturing; Dams; Emergency Services; and Nuclear Reactors, Materials, and Waste (Nuclear).

The mission of SOPD is to enhance the resiliency of the Nation by leading the unified public-private sector effort to ensure its assigned CIKR are prepared, more secure, and safer from terrorist attacks, natural disasters, and other incidents. To achieve this mission, SOPD leverages the resources and knowledge of its CIKR sectors to develop and apply security initiatives that result in significant, measurable benefits to the Nation.

Each SOPD branch builds sustainable partnerships with its public and private sector stakeholders to enable more effective sector coordination, information sharing, and program development and implementation. These partnerships are sustained through the Sector Partnership Model, described in the NIPP 2013 pages 10–12.

Information sharing is a key component of the NIPP Partnership Model, and DRS sponsored conferences are one mechanism for information sharing. To facilitate conference planning and organization, SOPD established an event registration tool for use by all of its branches. The information collection is voluntary and is used by the SSAs within the SOPD. The six SSAs within SOPD use this information to register public and private sector stakeholders for meetings hosted by the SSA. SOPD will use the information collected to reserve space at a meeting for the registrant; contact the registrant with a reminder about the event; develop meeting materials for attendees; determine key topics of interest; and efficiently generate attendee and speaker nametags. Additionally, it will allow SOPD to have a better understanding of the organizations participating in the CIKR

protection partnership events. By understanding who is participating, the SSA can identify portions of a sector that are underrepresented, and the SSA could then target that underrepresented sector elements through outreach and awareness initiatives.

Analysis

Agency: Department of Homeland Security, National Protection and Programs Directorate, Office of Infrastructure Protection, Sector Outreach and Programs Division.

Title: Sector Outreach and Programs Division Online Meeting Registration Tool.

OMB Number: 1670.

Frequency: Annually.

Affected Public: Federal, state, local, tribal, and territorial government personnel; private sector members.

Number of Respondents: 1000 respondents (estimate).

Estimated Time per Respondent: 3 minutes.

Total Burden Hours: 50 annual burden hours.

Total Burden Cost (capital/startup): $0.

Total Recordkeeping Burden: $7200.00.

Total Burden Cost (operating/maintaining): $8350.44.

Dated: April 28, 2014.

Scott Libby,

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

[FR Doc. 2014–10078 Filed 5–1–14; 8:45 am]

BILLING CODE 9110–9P–P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS–2014–0014]

President's National Security Telecommunications Advisory Committee

AGENCY: National Protection and Programs Directorate, DHS.

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

SUMMARY: The President's National Security Telecommunications Advisory Committee (NSTAC) will meet on Wednesday, May 21, 2014, in Washington, DC. The meeting will be partially closed to the public.

DATES: The NSTAC will meet in a closed session on Wednesday, May 21, 2014, from 9:15 a.m. to 11:15 a.m. and in an open session on Wednesday, May 21, 2014, from 12:45 p.m. to 4:00 p.m.

ADDRESSES: The open session will be held at the Eisenhower Executive Office Building, Washington, DC and will begin at 12:45 p.m. Seating is limited and therefore will be provided on a first-come,first-servebasis. Additionally, the public portion of the meeting will be streamed via webcast at *http://www.whitehouse.gov/live.* For information on facilities or services for individuals with disabilities or to request special assistance at the meeting, contact *nstac@dhs.gov* as soon as possible.

We are inviting public comment on the issues the NSTAC will consider, as listed in the **SUPPLEMENTARY INFORMATION** section below. Associated briefing materials that will be discussed at the meeting will be available at *www.dhs.gov/nstac* for review as of May 5, 2014. Comments must be submitted in writing no later than May 14, 2014. Comments must be identified by docket number DHS–2014–0014 and may be submitted by *one* of the following methods:

- Federal eRulemaking Portal: *http://www.regulations.gov.* Follow the instructions for submitting comments.
- Email: *NSTAC@dhs.gov.* Include the docket number in the subject line of the message.
- Fax: 703–235–5962, Attn: Sandy Benevides.
- Mail: Designated Federal Officer, National Security Telecommunications Advisory Committee, National Protection and Programs Directorate, Department of Homeland Security, 245 Murray Lane, Mail Stop 0615, Arlington VA 20598–0615.

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 NSTAC, go to *http://www.regulations.gov,* referencing docket number DHS–2014–0014.

A public comment period will be held during the open portion of the meeting on Wednesday, May 21, 2014, from 3:15 p.m. to 3:45 p.m., and speakers are requested to limit their comments to 3 minutes. Please note that the public comment period may end before the time indicated, following the last call for comments. Contact Sandy Benevides at 703–235–5408 or *Sandra.Benevides@dhs.gov* to register as a speaker by close of business on May 14, 2014. Speakers will be accommodated in order of registration within the constraints of the time allotted to public comment.

FOR FURTHER INFORMATION CONTACT: Helen Jackson, NSTAC Designated Federal Officer, Department of Homeland Security, telephone (703) 235–5321 or *Helen.Jackson@dhs.gov.*

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the Federal Advisory Committee Act, 5 U.S.C. App. (Pub. L. 92–463). The NSTAC advises the President on matters related to national security and emergency preparedness (NS/EP) telecommunications policy.

Agenda: The committee will meet in open session to engage in an international panel discussion comprised of members from Canada, the United Kingdom, and the United States to discuss their country's approaches to infrastructure protection. Additionally, members will receive feedback from the Department of Homeland Security regarding the progress of the Government's implementation of recent NSTAC recommendations. The NSTAC members will be briefed on the committee's progress regarding its report on the Internet of Things. The committee will examine the cybersecurity implications of the Internet of Things, within the context of national security and emergency preparedness. Finally, NSTAC members will deliberate and vote on the *NSTAC Information Technology Mobilization Scoping Report.* The NSTAC will meet in a closed session to hear a classified briefing regarding cybersecurity threats and to discuss future studies based on Government's security priorities and perceived vulnerabilities.

Basis for Closure: In accordance with 5 U.S.C. 552b(c), *Government in the Sunshine Act,* it has been determined that two agenda items require closure as the disclosure of the information would not be in the public interest.

The first of these agenda items, the classified briefing, will provide members with context on nation state capabilities and strategic threats. Such threats target national communications infrastructure and impact industry's long-term competitiveness and growth, as well as the Government's ability to mitigate threats. Disclosure of these threats would provide criminals who wish to intrude into commercial and Government networks with information on potential vulnerabilities and mitigation techniques, also weakening existing cybersecurity defense tactics. This briefing will be classified at the top secret level, thereby exempting disclosure of the content by statute. Therefore, this portion of the meeting is