9110-9P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2016-0065]

The President's National Security Telecommunications Advisory Committee

AGENCY: Department of Homeland Security

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, December 7, 2016, in Washington, D.C. The meeting will be partially closed to the public.

DATE: The NSTAC will meet on Wednesday, December 7, 2016, from 9:00 a.m. to 3:20 p.m. Eastern Standard Time (EST). Please note that the meeting may close early if the committee has completed its business.

ADDRESSES: The December 2016 NSTAC Meeting's open session will be held at the Eisenhower Executive Office Building, Washington, DC. Due to limited seating, requests to attend in person will be on a first-come basis and the public portion of the meeting will be streamed via webcast at http://www.whitehouse.gov/live, as an alternative option. Individuals who intend to participate in the meeting will need to register by sending an email to NSTAC@hq.dhs.gov by 5:00 p.m. EST on Wednesday, November 30, 2016. For information on facilities or services for individuals with disabilities, or to request special assistance at the meeting, please contact NSTAC@hq.dhs.gov as soon as possible.

Members of the public are invited to provide comment on the issues to be considered by the committee as listed in the SUPPLEMENTARY INFORMATION section below. Associated briefing materials to be discussed at the meeting will be available at www.dhs.gov/nstac for review on Monday, November 21, 2016. Comments may be submitted at any time and must be identified by docket number DHS-2016-0065. Comments may be submitted by one of the following methods:

- **Federal eRulemaking Portal:** http://www.regulations.gov. Please follow the instructions for submitting written comments.
- **Email:** NSTAC@hq.dhs.gov. Include the docket number DHS-2016-0065 in the subject line of the email message.
- **Fax:** (703) 235-5962, ATTN: Sandy Benevides.
- **Mail:** Designated Federal Officer, Stakeholder Engagement and Critical Infrastructure Resilience Division, National Protection and Programs Directorate, Department of Homeland Security, 245 Murray Lane, Mail Stop 0604, Arlington, VA 20598-0604.

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 www.regulations.gov, including any personal information provided.

Docket: For access to the docket and comments received by the NSTAC, please go to www.regulations.gov and enter docket number DHS-2016-0065.

A public comment period will be held during the meeting from 2:50 p.m. to 3:20 p.m. Speakers who wish to participate in the public comment period must register in advance and can do so by emailing NSTAC@hq.dhs.gov no later than Friday,

December 2, 2016, at 5:00 p.m. EST. Speakers are requested to limit their comments to three minutes. Please note that the public comment period may end before the time indicated, following the last call for comments.

FOR FURTHER INFORMATION CONTACT: Helen Jackson, NSTAC Designated Federal Officer, Department of Homeland Security, (703) 235-5321 (telephone) or helen.jackson@hq.dhs.gov (email).

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the Federal Advisory Committee Act, 5 U.S.C. appendix (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 an open session on December 7, 2016, to receive remarks from Department of Homeland Security (DHS) leadership and other senior Government officials regarding the Government's current cybersecurity initiatives and NS/EP priorities. Meeting participants will: (1) receive a keynote address regarding the Government's ongoing cybersecurity and NS/EP communications efforts; (2) engage in a panel discussion with senior Government officials regarding the effects of new technology on NS/EP processes and procedures; and (3) discuss the progress related to the draft National Cyber Incident Response Plan. Additionally, DHS will provide NSTAC members an update on the Government's progress in implementing recent NSTAC recommendations. Finally, the NSTAC members will receive an update on the NSTAC Emerging Technologies Strategic Vision Subcommittee's study of the near- and long-term NS/EP implications of emergent and expected information and communications technologies.

The committee will also meet in a closed session to receive a classified briefing regarding cybersecurity threats and discuss future studies based on the Government's NS/EP priorities and perceived vulnerabilities.

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

The first of these agenda items, the classified briefing, will provide members with a cybersecurity threat briefing on threats to critical infrastructure. Disclosure of these threats would provide criminals who seek to compromise commercial and Government networks with information on potential vulnerabilities and mitigation techniques, weakening the Nation's cybersecurity posture. This briefing will be classified at the top secret/sensitive compartmented information level, thereby exempting disclosure of the content by statute. Therefore, this portion of the meeting is required to be closed pursuant to 5 U.S.C. 552b(c)(1)(A) & (B).

The second agenda item, the discussion of potential NSTAC study topics, will address areas of critical cybersecurity vulnerabilities and priorities for Government. Government officials will share data with NSTAC members on initiatives, assessments, and future security requirements across public and private sector networks. The information will include specific vulnerabilities within cyberspace that affect the United States' ICT infrastructures and proposed mitigation strategies. Disclosure of this information to the public would provide criminals with an incentive to focus on these vulnerabilities to increase attacks on the Nation's critical infrastructure and communications networks. As disclosure of this portion of the meeting is likely to

significantly frustrate implementation of proposed DHS actions, it is required to be closed pursuant to 5 U.S.C. 552b(c)(9)(B).

Dated: November 9, 2016.

Helen Jackson,
Designated Federal Officer for the NSTAC.
[FR Doc. 2016-27572 Filed: 11/15/2016 8:45 am; Publication Date: 11/16/2016]