

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-serve basis. 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](mailto: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](http://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](mailto: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](mailto: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](mailto: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

required to be closed pursuant to 5 U.S.C. 552b(c)(1)(A).

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. The data to be shared includes specific vulnerabilities within cyberspace that affect the Nation's communications and information technology 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 our cyber and communications networks. Therefore, this portion of the meeting is likely to significantly frustrate implementation of proposed DHS actions and is required to be closed pursuant to 5 U.S.C. 552b(c)(9)(B).

Dated: April 25, 2014.

**Helen Jackson,**

*Designated Federal Officer for the NSTAC.*

[FR Doc. 2014-10024 Filed 5-1-14; 8:45 am]

**BILLING CODE P**

## DEPARTMENT OF HOMELAND SECURITY

### Coast Guard

[USCG-2013-0316]

### Outer Continental Shelf Units—Fire and Explosion Analyses

**AGENCY:** Coast Guard, DHS.

**ACTION:** Notice of recommended interim voluntary guidelines.

**SUMMARY:** As part of its continuing response to the explosion, fire and sinking of the mobile offshore drilling unit (MODU) *DEEPWATER HORIZON* in the Gulf of Mexico on April 20, 2010, the Coast Guard is providing recommended interim voluntary guidelines concerning fire and explosion analyses for MODUs and manned fixed and floating offshore facilities engaged in activities on the U.S. Outer Continental Shelf (OCS). **DATES:** The recommended voluntary guidelines in this notice are effective May 2, 2014.

Documents mentioned as being available in the docket are part of docket USCG-2013-0316 and are available for inspection or copying at the Docket Management Facility (M-30), U.S. Department of Transportation, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE.,

Washington, DC 20590, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. You may also find this docket on the Internet by going to <http://www.regulations.gov>, inserting USCG-2013-0316 in the "Keyword" box, and then clicking "Search."

**FOR FURTHER INFORMATION CONTACT:** If you have questions on this notice, call or email LCDR John H. Miller, U.S. Coast Guard, Office of Design and Engineering Standards, Lifesaving and Fire Safety Division (CG-ENG-4), telephone (202) 372-1372, email [John.H.Miller@uscg.mil](mailto:John.H.Miller@uscg.mil).

### Background

The "Report of Investigation into the Circumstances Surrounding the Explosion, Fire, Sinking and Loss of Eleven Crew Members Aboard the Mobile Offshore Drilling Unit (MODU) *DEEPWATER HORIZON* in the Gulf of Mexico, April 20-22, 2010," (hereinafter referred to as "Report"), and related Commandant's Final Action Memo, dated September 9, 2011, contain a number of recommendations for OCS safety improvements that are presently being evaluated for further regulatory action. (These documents may be found in the docket for this action, as indicated under ADDRESSES).

Recommendations 1D, 1E, 2B, 2C, 2E, and 3A in the Report urged the Coast Guard to evaluate the need for fire and explosion risk analyses to ensure an adequate level of protection is provided for accommodation spaces, escape paths, embarkation stations, and structures housing vital safety equipment from drill floor and production area events. The Report highlighted the following considerations as areas not specifically addressed by current regulations:

- Minimum values are needed for explosion design loads for use in calculating the required blast resistance of structures;
- Explosion risk analysis of the design and layout of each facility should be performed to identify high risk situations;
- H-60 rated fire boundaries between the drilling area and adjacent accommodation spaces and spaces housing vital safety equipment may be necessary dependent on the arrangement of the facility;
- Uniform guidelines for performing engineering evaluations to ensure adequate protection of bulkheads and decks separating hazardous areas from adjacent structures and escape routes for likely drill floor fire scenarios are necessary;
- Performance-based fire risk analysis should be used to supplement the

prescriptive requirements in the MODU Code; such analysis should use defined heat flux loads to calculate necessary levels of protection for structures, equipment, and vital systems that could be affected by fires on the drill floor;

- Maximum allowable radiant heat exposure limits for personnel at the muster stations and lifesaving appliance launching stations in anticipated evacuation scenarios should be implemented.

To implement these recommendations, a future Coast Guard rulemaking will address fire and explosion risk analyses for MODUs and manned fixed and floating offshore facilities engaged in OCS activities. Comments will be invited in connection with that rulemaking.

Currently, there is no requirement in the current OCS regulations, in Title 33 of the Code of Federal Regulations (CFR), that requires a fire and explosion analysis that would implement the recommendations from the Report. Furthermore, while Section 9 of the 2009 IMO MODU Code contains some recommendations on the parameters of fire and explosion risk analysis, we believe that these recommendations are not sufficiently specific to adequately and consistently address these recommendations from the Report on their own.

We believe that the recommendations from the 2009 IMO MODU Code are insufficiently specific for several reasons. Section 9.3.1 of the 2009 MODU Code provides, "In general, accommodation spaces, service spaces and control stations should not be located adjacent to hazardous areas. However, where this is not practicable, an engineering evaluation should be performed to ensure that the level of fire protection and blast resistance of the bulkheads and decks separating these spaces from the hazardous areas are adequate for the likely hazard." This requirement is not specific enough to consistently ensure the protection of safety-critical spaces and elements aboard MODUs and manned fixed and floating offshore facilities engaged in OCS activities, and needs to be supported by guidance to better define what the "engineering evaluation" should include and what performance criteria should be met to ensure "adequate protection" is provided. Safety-critical spaces and elements refers to any accommodation or work area, equipment, system, device, or material, the failure, destruction, or release of which could directly or indirectly endanger the survivability of the facility and the personnel onboard. These safety-critical spaces and