

Cancer Control, National Institutes of Health, HHS)

Dated: December 8, 2014.

Melanie J. Gray,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2014-29161 Filed 12-11-14; 8:45 am]

BILLING CODE 4140-01-P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Institute of Allergy and Infectious Diseases; Notice of Closed Meeting

Pursuant to section 10(d) of the Federal Advisory Committee Act, as amended (5 U.S.C. App.), notice is hereby given of the following meeting.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: National Institute of Allergy and Infectious Diseases Special Emphasis Panel; NIAID SBIR Phase II Clinical Trial Implementation Cooperative Agreement (U44).

Date: January 6, 2015.

Time: 1:00 p.m. to 4:00 p.m.

Agenda: To review and evaluate grant applications.

Place: 5601 Fishers Lane, Room 3G62, Rockville, MD 20852, (Telephone Conference Call).

Contact Person: Travis J. Taylor, Ph.D., Scientific Review Program DEA/NIAID/NIH/DHHS, 5601 Fishers Lane, Rockville, MD 20852, 240-669-5082, Travis.Taylor@nih.gov.

(Catalogue of Federal Domestic Assistance Program Nos. 93.855, Allergy, Immunology, and Transplantation Research; 93.856, Microbiology and Infectious Diseases Research, National Institutes of Health, HHS)

Dated: December 8, 2014.

David Clary,

Program Analyst, Office of Federal Advisory Committee Policy.

[FR Doc. 2014-29160 Filed 12-11-14; 8:45 am]

BILLING CODE 4140-01-P

DEPARTMENT OF HOMELAND SECURITY

[Docket No. DHS-2014-0007]

Critical Infrastructure Private Sector Clearance Program Request (CI PSCP)

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: 30-day notice and request for comments; new information collection request: 1670-0013.

SUMMARY: The Department of Homeland Security (DHS), National Protection and Programs Directorate (NPPD), Office of Infrastructure Protection (IP) 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). DHS previously published this Information Collection Request (ICR) in the **Federal Register** on September 24, 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 January 12, 2015. This process is conducted in accordance with 5 CFR 1320.10.

ADDRESSES: Written comments and questions about this ICR should be forwarded to DHS/NPPD/IP/Attn: Cheryl Fenoli, 245 Murray Lane SW., Mail Stop 0607, Arlington, VA 20598-0609. Email requests should go to Cheryl Fenoli, Cheryl.Fenoli@hq.dhs.gov. Written comments should reach the contact person listed no later than January 12, 2015. Comments must be identified by "DHS-2014-0007" and may be submitted by one of the following methods:

- **Federal eRulemaking Portal:** <http://www.regulations.gov>.

- **Email:** Include the docket number in the subject line of the message.

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.

SUPPLEMENTARY INFORMATION: The CI PSCP sponsors clearances for private-sector partners who are responsible for critical infrastructure protection in accordance with Executive Order 13549. The PSCP requires individuals to complete a clearance request form that initiates the clearance process. Sector Specific Agencies (SSAs), NPPD/IP

Protective Security Advisors, Sector Liaisons, the National Infrastructure Coordinating Center, and other federal officials designated by NPPD/IP are authorized to submit nominations to the central PSCP point of contact, the PSCP Administrator. The clearance request form is signed by both the federal official who nominated the applicant and by the Assistant Secretary for IP prior to initiating the clearance process. Upon approval by the Assistant Secretary for IP, IP Security Office will contact the nominee to obtain the social security number, date and place of birth, and will then enter this data into e-QIP—Office of Personnel Management's secure portal for investigation processing. Once the data is entered in e-QIP, the applicant can complete the online security questionnaire. An alternate mailing address is an optional field on the form and may be provided if the nominee chooses to have correspondences sent to a mailing address other than the company mailing address. The IP Security Office maintains all applicants' information in the Master Roster, which contains all the information found on the clearance request form in addition to their clearance information (date granted, level of clearance, date non-disclosure agreements signed, and type/date of investigation). The Administrator of the Master Roster maintains the information so as to track clearance processing and investigation information and to have the most current contact information for the participants from each sector.

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.

Analysis

Agency: Department of Homeland Security, National Protection and

Programs Directorate, Office of Infrastructure Protection.

Title: Critical Infrastructure Private Sector Clearance Program Request.

OMB Number: 1670-0013.

Frequency: Once.

Affected Public: Designated private sector employees of critical infrastructure entities or organizations.

Number of Respondents: 500 respondents (estimate).

Estimated Time per Respondent: 10 minutes.

Total Burden Hours: 83.35.

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

Total Recordkeeping Burden: \$0.

Total Burden Cost (operating/maintaining): \$0.

Dated: December 8, 2014.

David Epperson,

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

[FR Doc. 2014-29175 Filed 12-11-14; 8:45 am]

BILLING CODE 9110-9P-P

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG-2014-1020]

Guidance on Maritime Cybersecurity Standards

AGENCY: Coast Guard, DHS.

ACTION: Notice of public meeting and request for comments.

SUMMARY: The U.S. Coast Guard announces a public meeting to be held in Washington, DC, to receive comments on the development of cybersecurity assessment methods for vessels and facilities regulated by the Coast Guard. This meeting will provide an opportunity for the public to comment on development of security assessment methods that assist vessel and facility owners and operators identify and address cybersecurity vulnerabilities that could cause or contribute to a Transportation Security Incident. The Coast Guard will consider these public comments in developing relevant guidance, which may include standards, guidelines, and best practices to protect maritime critical infrastructure.

DATES: The meeting will be held on Thursday, January 15, 2015 from 9:00 a.m. to 12:00 p.m. The deadline to reserve a seat is Monday, January 5, 2015. All written comments and related material must either be submitted to the online docket via <http://www.regulations.gov> on or before

January 29, 2015 or reach the Docket Management Facility by that date.

ADDRESSES: The public meeting will be held at the Department of Transportation Headquarters, Oklahoma Room, 1200 New Jersey Avenue SE., Washington, DC 20590; the building telephone number is 202-366-1035. The building is accessible by taxi, public transit, and privately-owned conveyance. However, public parking in the vicinity of the building is extremely limited. Meeting participants are encouraged to use mass transit.

Seating is limited, so please reserve a seat as soon as possible, but no later than January 5, 2015. To reserve a seat, please email Josephine.A.Long@uscg.mil with the participant's first and last name for all U.S. Citizens, and additionally, official title, date of birth, country of citizenship, and passport number with expiration date for non-U.S. Citizens. To gain entrance to the Department of Transportation Headquarters building, all meeting participants must present government-issued photo identification (e.g., state-issued driver's license). If a visitor does not have a photo ID, that person will not be permitted to enter the facility. All visitors and any items brought into the facility will be required to go through security screening each time they enter the building.

The Coast Guard will provide a live video feed of the meeting. To access the video feed, email a request to LT Josephine Long at Josephine.A.Long@uscg.mil no later than January 13, 2015.

The docket for this notice is 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>, entering USCG-2014-1020 in the search box and following the instructions.

Written comments may also be submitted in response to this notice. All written comments and related material submitted before or after the meeting must either be submitted to the online docket via <http://www.regulations.gov> on or before January 29, 2015 or reach the Docket Management Facility by that date. You may submit written comments identified by docket number USCG-2014-1020 before or after the meeting using any one of the following methods:

- (1) Federal eRulemaking Portal: <http://www.regulations.gov>.
- (2) Fax: 202-372-1990.
- (3) Mail: Docket Management Facility (M-30), U.S. Department of

Transportation, West Building Ground Floor, Room W12-140, 1200 New Jersey Avenue SE., Washington, DC 20590-0001.

(4) Hand delivery: Same as mail address above, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.

To avoid duplication, please use only one of these four methods.

The Coast Guard will post a video recording and written summary of the meeting to the docket.

FOR FURTHER INFORMATION CONTACT: If there are questions concerning this meeting, please call or email LT Josephine Long, Coast Guard at 202-372-1109 or via email at Josephine.A.Long@uscg.mil or LCDR Joshua Rose, Coast Guard; at 202-372-1106 or via email at Joshua.D.Rose@uscg.mil. If there are questions on viewing or submitting material to the docket, call Ms. Cheryl Collins, Program Manager, Docket Operations, telephone 202-366-9826.

SUPPLEMENTARY INFORMATION:

Background and Purpose

On February 12, 2013, the President signed Executive Order (E.O.) 13636 "Improving Critical Infrastructure Cybersecurity." The E.O. provided the national approach to protecting critical infrastructure cybersecurity and directed federal agencies to assess cyber risk to critical infrastructure. Pursuant to E.O. 13636, the National Institute of Standards and Technology (NIST) developed a voluntary Preliminary Cybersecurity Framework,¹ followed by the February 12, 2014 publication of a Framework for Improving Critical Infrastructure Cybersecurity² (Cybersecurity Framework). The Cybersecurity Framework serves to help industry stakeholders reduce their cyber risk and vulnerabilities. The Coast Guard encourages vessel and facility owners and operators to adopt the Cybersecurity Framework voluntarily to achieve a minimum standard of cybersecurity protection.

Section 7(d) of E.O. 13636 states that in developing the Cybersecurity Framework, the Director of NIST "shall engage in an open public review and comment process" and consult with stakeholders including owners and operators of critical infrastructure.

¹ The Preliminary Cybersecurity Framework is available for viewing online at <http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf>.

² The Framework for Improving Critical Infrastructure Cybersecurity is available for viewing online at <http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf>.