DEPARTMENT OF HOMELAND SECURITY

Coast Guard

[Docket No. USCG–2016–0122]

Merchant Mariner Medical Advisory Committee

AGENCY: Coast Guard, Department of Homeland Security.

ACTION: Notice of Federal Advisory Committee meeting.

SUMMARY: The Merchant Mariner Medical Advisory Committee and its working groups will meet to discuss matters relating to medical certification determinations for issuance of licenses, certificates of registry, merchant mariners' documents, medical standards and guidelines for the physical qualifications of operators of commercial vessels, medical examiner education, and medical research. The meetings will be open to the public.

DATES: The Merchant Mariner Medical Advisory Committee and its working groups are scheduled to meet on Monday, March 14 and Tuesday, March 15, 2016, from 8 a.m. to 5:15 p.m. and 8 a.m. to 5 p.m. Please note that these meetings may adjourn early if the committee has completed its business.

ADDRESSES: The meetings will be held at the Crowley Maritime Corporation, 1st Floor Conference Room, 9487 Regency Square Blvd., Jacksonville, FL 32225 (*http://www.crowley.com*). For further information about the meeting facilities, please contact Ms. Becky Kelly at (904)727–4213.

Please be advised that all attendees are required to check-in to the visitor's booth located to the right of the main building entrance. All attendees will be required to provide a government-issued picture identification card in order to gain admittance to the building. For planning purposes, please notify the Merchant Mariner Medical Advisory Committee Alternate Designated Federal Officer of your attendance as soon as possible using the contact information provided in the **FOR FURTHER INFORMATION CONTACT** section of this notice.

For information on facilities or services for individuals with disabilities or to request special assistance at the meeting, contact the Alternate Designated Federal Officer as soon as possible.

To facilitate public participation, we are inviting public comment on the issues to be considered by the committee as listed in the ''Agenda'' section below. Written comments for distribution to committee members must be submitted no later than March 7, 2016, if you want the committee members to be able to review your comments before the meeting, and must be identified by docket number USCG–2016–0122. Written comments may be submitted using the Federal eRulemaking Portal: *http://www.regulations.gov.* If your material cannot be submitted using *http://www.regulations.gov,* contact the person in the Alternate Designated Federal Officer for alternate instructions.

Instructions: All submissions 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. You may review a Privacy Act notice regarding the Federal Docket Management System in the March 24, 2005 issue of the **Federal Register** (70 FR 15086).

Docket: For access to the docket to read documents or comments related to this Notice, go to *http://www.regulations.gov,* insert USCG–2016–0122 in the ''SEARCH'' box, press Enter and then click on the item you wish to view.

A public comment period will be held on March 14, 2016, from approximately 11:30 a.m.–12 p.m. and March 15, 2016 from approximately 2:15 p.m.–2:45 p.m. Speakers are requested to limit their comments to 5 minutes. Please note that the public comment period may end before the time indicated, following the last call for comments. Additionally, public comment will be sought throughout the meeting as specific issues are discussed by the committee. Contact Lieutenant Ashley Holm as indicated below to register as a speaker.

FOR FURTHER INFORMATION CONTACT: Lieutenant Ashley Holm, Alternate Designated Federal Officer for the Merchant Mariner Medical Advisory Committee, 2703 Martin Luther King Jr. Ave SE., Stop (7501), telephone 202–372–1128, fax 202–372–4908 or *Ashley.e.holm@uscg.mil.*

SUPPLEMENTARY INFORMATION: Notice of this meeting is given under the *Federal Advisory Committee Act,* Title 5 United States Code Appendix. The Merchant Mariner Medical Advisory Committee Meeting is authorized by 46 United States Code 7115 and advises the Secretary on matters related to (a) medical certification determinations for issuance of licenses, certificates of registry, and merchant mariners' documents; (b) medical standards and guidelines for the physical qualifications of operators of commercial vessels; (c) medical examiner education; and (d) medical research.

Agenda

Day 1

The agenda for the March 14, 2016 meeting is as follows:

(1) Opening remarks from Crowley Maritime leadership.

(2) Opening remarks from Coast Guard leadership.

(3) Opening remarks from the Designated Federal Officer.

(4) Roll call of committee members and determination of a quorum.

(5) Review of last full committee meeting's minutes.

(6) Introduction of new task(s).

(7) Presentation and discussion on marine casualty investigations and data analysis (could lead to future tasking for the committee).

(8) Public comment period.

(9) Presentation on mariner wellness.

(10) Working Groups addressing the following task statements may meet to deliberate–

(a) Task statement 13, Mariner Occupational Health Risk Analysis. This is a joint task statement with the Merchant Marine Personnel Advisory Committee.

(b) Task statement(s) requesting recommendations on training content for a Designated Medical Examiner program.

(c) Task statement requesting recommendations on guidance to mariners on over the counter medications, energy drinks/pills, diet aids, and dietary supplements.

(d) The Committee may receive new task statements from the Coast Guard, review the information presented on each issue, deliberate and formulate recommendations for the Department's consideration.

(10) Adjournment of meeting.

Day 2

The agenda for the March 15, 2016 meeting is as follows:

(1) Continue work on Task Statements.

(2) Presentation from the Council on Chiropractic Education.

(3) Public comment period.

(4) By mid-afternoon, the Working Groups will report, and if applicable, make recommendations for the full committee to consider for presentation to the Coast Guard. The committee may vote on the working group's recommendations on this date. The public will have an opportunity to speak after each Working Group's Report before the full committee takes any action on each report.

(5) Closing remarks/plans for next meeting.

(6) Adjournment of Meeting.

Dated: February 11, 2016.

V.B. Gifford,

Captain, U.S. Coast Guard, Director of Inspections and Compliance.

[FR Doc. 2016–03348 Filed 2–17–16; 8:45 am]

BILLING CODE 9110–04–P

DEPARTMENT OF HOMELAND SECURITY

National Protection and Programs Directorate; Cybersecurity Information Sharing Act of 2015 Interim Guidance Documents—Notice of Availability

AGENCY: National Protection and Programs Directorate, DHS.

ACTION: Notice of availability.

SUMMARY: DHS is announcing the availability of Cybersecurity Information Sharing Act of 2015 Interim Guidance Documents jointly issued with the Department of Justice (DOJ) in compliance with the Act (CISA), which authorizes the voluntary sharing and receiving of cyber threat indicators and defensive measures for cybersecurity purposes, consistent with certain protections, including privacy and civil liberty protections.

ADDRESSES: The CISA guidance documents may be found on *www.us-cert.gov/ais.*

FOR FURTHER INFORMATION CONTACT: If you have questions about this notice, email Matthew Shabat at *matthew.shabat@hq.dhs.gov* or telephone on (703) 235–5338. Questions may also be directed by mail to Matthew Shabat, 245 Murray Lane SW., Mail Stop 0610, Washington, DC 20528–0610.

SUPPLEMENTARY INFORMATION: The CISA requires the Secretary of DHS and the Attorney General to jointly develop and make publicly available—

- guidance to assist non-Federal entities and promote sharing of cyber threat indicators with the Federal Government;
- interim and final guidelines for the protection of privacy and civil liberties; and
- interim and final procedures related to the receipt of cyber threat indicators and defensive measures by the Government, which happen principally through the real-time DHS process, the existing DHS-operated Automated Indicator Sharing (AIS) initiative and may also occur through direct submissions to Federal agencies.

The CISA also requires the Secretary of DHS, the Attorney General, the Director of National Intelligence, and the Secretary of Defense, to jointly develop interim procedures to facilitate and promote the sharing of cyber threat indicators and defensive measures by the Federal Government.

Authority and Background

On December 18, 2015, the President signed into law the Consolidated Appropriations Act, 2016, Public Law 114–113, which included at Division N, Title I the Cybersecurity Information Sharing Act of 2015 (CISA). Congress designed CISA to establish a voluntary cybersecurity information sharing process that encourages public and private sector entities to share cyber threat indicators and defensive measures while protecting privacy and civil liberties. The CISA requires various Executive Branch agencies to coordinate and create, within 60 days of enactment (*i.e.*, not later than February 16, 2016), four guidance documents to facilitate this voluntary cybersecurity information sharing process. The CISA requires two of these interim documents to be made publicly available. *See generally* Public Law 114–113, Div. N, Title I secs. 103, 105).

Overview of the 60 Day Guidance Required Under CISA

The CISA sec. 103 requires the Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of designated Federal entities,[1] to jointly develop and issue procedures to facilitate and promote the sharing by the Federal Government of classified and unclassified cyber threat indicators, defensive measures, and other information and best practices related to mitigating cyber threats. The CISA sec. 103(b) requires these procedures to include a real-time sharing capability (namely the DHS Automated Indicator Sharing (AIS) initiative); incorporate existing Federal information sharing processes, procedures, roles, and responsibilities to the greatest extent possible; account for sharing done in error; and protect against unauthorized access to cyber threat information. Further, the procedures must account for the review of cyber threat indicators to identify personal information not related to the threat, a technical capability to remove such personal information, and a notification process to alert any U.S. person whose personal information is improperly shared by a Federal entity.

The CISA sec. 105(a)(1) requires the Secretary of Homeland Security and the Attorney General, in consultation with the heads of designated Federal entities, to jointly develop and issue interim policies and procedures relating to the receipt of cyber threat indicators and defensive measures by the Federal Government. These internal operational procedures describe general rules applicable to DHS and other Federal agencies and the operative processes of the DHS AIS system, including the statutory requirement for Federal agencies that receive cyber threat indicators and defensive measures to share them with other appropriate agencies.

The CISA sec. 105(a)(4) requires the Secretary of Homeland Security and the Attorney General to jointly develop and make publicly available guidance to assist non-Federal entities with sharing cyber threat indicators with Federal entities. This guidance includes explanations of how non-Federal entities can identify and share cyber threat indicators and defensive measures with the Federal Government in accordance with CISA and describes the protections non-Federal entities receive under CISA for sharing cyber threat indicators and defensive measures, including targeted liability protection and other statutory protections.

Finally, CISA sec. 105(b) requires the Secretary of Homeland Security and the Attorney General, in consultation with the Department Heads and Chief Privacy and Civil Liberties Officers of the designated Federal entities, to jointly develop and make publicly available interim guidelines relating to privacy and civil liberties that govern the receipt, retention, use, and dissemination of cyber threat indicators by a Federal entity. These privacy and civil liberties guidelines are consistent with the Fair Information Practice Principles (FIPPs) set forth in Appendix A of the ''National Strategy for Trusted Identities in Cyberspace,'' published by the President in April 2011.

Issuance of Agency Guidance Required Under CISA

The CISA guidance documents may be found on *www.us-cert.gov/ais.*

Dated: February 11, 2016.

Andy Ozment,

Assistant Secretary, Department of Homeland Security.

[FR Doc. 2016–03430 Filed 2–17–16; 8:45 am]

BILLING CODE 9110–9P–P

[1] The CISA defines *Appropriate Federal Entities* as the Departments of Commerce, Defense, Energy, Homeland Security, Justice, Treasury, and the Office of the Director of National Intelligence. *See* CISA sec. 102(3).