

**POLICIES AND PRACTICES FOR STORING, RETRIEVING, ACCESSING, RETAINING, AND DISPOSING OF RECORDS IN THE SYSTEM:**

**STORAGE**

Records in this system are on paper and/or in digital or other electronic form. Digital and other electronic images are stored on a storage area network in a secured environment.

**RETRIEVABILITY:**

Information may be retrieved by an identification number assigned by computer, by facility, by business affiliation, e-mails address, or by the name of the individual.

**SAFEGUARDS:**

Information in this system is safeguarded in accordance with applicable laws, rules and policies, including the DHS Information Technology Security Program Handbook. Further, GITAARS security protocols will meet multiple NIST Security Standards from Authentication to Certification and Accreditation. Records in the GITAARS will be maintained in a secure, password protected electronic system that will utilize security hardware and software to include: multiple firewalls, active intruder detection, and role-based access controls. Additional safeguards will vary by component and program. All records are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include: restricting access to authorized personnel who have a "need to know;" using locks; and password protection identification features. Classified information is appropriately stored in accordance with applicable requirements. DHS file areas are locked after normal duty hours and the facilities are protected from the outside by security personnel.

**RETENTION AND DISPOSAL:**

Records are retained and disposed of in accordance with the National Archives and Records Administration's General Records Schedule 24, section 6, "User Identification, Profiles, Authorizations, and Password Files." Inactive records will be destroyed or deleted 6 years after the user account is terminated or password is altered, or when no longer needed for investigative or security purposes, whichever is later.

**SYSTEM MANAGER(S) AND ADDRESS:**

For Headquarters components of the Department of Homeland Security, the System Manager is the Director of Departmental Disclosure, U.S. Department of Homeland Security, Washington, DC 20528.

For operational components that comprise the U.S. Department of Homeland Security, the System Managers are as follows:

- United States Coast Guard, FOIA Officer/PA System Manager, Commandant, CG-611, U.S. Coast Guard, 2100 2nd Street, SW., Washington, DC 20593-0001.
- United States Secret Service, FOIA/PA System Manager, Suite 3000, 950 H Street, NW., Washington, DC 20223.
- Under Secretary for Federal Emergency Management Directorate, FOIA/PA System Manager, 500 C Street, SW., Room 840, Washington, DC 20472.
- Director, Citizenship and Immigration Services, U.S. Citizenship and Immigration Services, ATTN: Records Services Branch (FOIA/PA), 111 Massachusetts Ave, NW., 2nd Floor, Washington, DC 20529.
- Commissioner, Customs and Border Protection, FOIA/PA System Manager, Disclosure Law Branch, Office of Regulations & Rulings, Ronald Reagan Building, 1300 Pennsylvania Avenue, NW., (Mint Annex) Washington, DC 20229.
- Bureau of Immigration and Customs Enforcement, FOIA/PA System Manager, Office of Investigation, Chester Arthur Building (CAB), 425 I Street, NW., Room 4038, Washington, DC 20538.
- Assistant Secretary, Transportation Security Administration, FOIA/PA System Manager, Office of Security, West Building, 4th Floor, Room 432-N, TSA-20, 601 South 12th Street, Arlington, VA 22202-4220.
- Federal Protective Service, FOIA/PA System Manager, 1800 F Street, NW., Suite 2341, Washington, DC 20405.
- Federal Law Enforcement Training Center, Disclosure Officer, 1131 Chapel Crossing Road, Building 94, Glynco, GA 31524.
- Under Secretary for Science & Technology, FOIA/PA System Manager, Washington, DC 20528.
- Under Secretary for Preparedness, Nebraska Avenue Complex, Building 81, 1st floor, Washington, DC 20528.
- Director, Operations Coordination, Nebraska Avenue Complex, Building 3, Washington, DC 20529.
- Officer of Intelligence and Analysis, Nebraska Avenue Complex, Building 19, Washington, DC 20529.

**NOTIFICATION PROCEDURE:**

To determine whether this system contains records relating to you, write to the appropriate System Manager(s) identified above.

**RECORD ACCESS PROCEDURES:**

A request for access to records in this system may be made by writing to the System Manager, identified above, in conformance with 6 CFR Part 5, Subpart B, which provides the rules for requesting access to Privacy Act records maintained by DHS.

**CONTESTING RECORD PROCEDURES:**

Same as "Records Access Procedures" above.

**RECORD SOURCE CATEGORIES:**

Information contained in this system is obtained from affected individuals/ organizations/facilities, public source data, other government agencies and/or information already in other DHS records systems.

**EXEMPTIONS CLAIMED FOR THE SYSTEM:**

None.

Dated: December 18, 2006.

**Hugo Teufel III,**

*Chief Privacy Officer.*

[FR Doc. E6-22008 Filed 12-28-06; 8:45 am]

**BILLING CODE 4410-10-P**

**DEPARTMENT OF HOMELAND SECURITY**

**Coast Guard**

[CGD01-06-133]

**Area Maritime Security Committee, Southeastern New England; Vacancies**

**AGENCY:** Coast Guard, DHS.

**ACTION:** Request for applications.

**SUMMARY:** The Coast Guard seeks applications for membership in the Area Maritime Security Committee, Southeastern New England. The Committee assists the Captain of the Port, Southeastern New England, in developing, reviewing, and updating the Area Maritime Security Plan for their area of responsibility.

**DATES:** Requests for membership should reach the Captain of the Port, Southeastern New England, on 19 January 2006.

**ADDRESSES:** Submit applications for membership to the Captain of the Port, Southeastern New England, U.S. Coast Guard Sector Southeastern New England, Contingency Planning and Force Readiness Department, 20 Risho Ave Unit D, East Providence, RI 02914-1208.

**FOR FURTHER INFORMATION CONTACT:** Mr. Peter Popko, 401-435-2380.

**SUPPLEMENTARY INFORMATION:**

### The Committee

The Area Maritime Security Committee, Southeastern New England (AMSC), is established under, and governed by, 33 CFR part 103, subpart C. The functions of the Committee include, but are not limited to, the following:

- (1) Identifying critical port infrastructure and operations.
- (2) Identifying risks (i.e., threats, vulnerabilities, and consequences).
- (3) Determining strategies and implementation methods for mitigation.
- (4) Developing and describing the process for continuously evaluating overall port security by considering consequences and vulnerabilities, how they may change over time, and what additional mitigation strategies can be applied.
- (5) Advising and assisting the Captain of the Port in developing, reviewing, and updating the Area Maritime Security Plan under 33 CFR part 103, subpart E.

### Positions Available on the Committee

There are 2 vacancies on the Committee. Members may be selected from—

- (1) The Federal, Territorial, or Tribal government;
- (2) The State government and political subdivisions of the State;
- (3) Local public safety, crisis management, and emergency response agencies;
- (4) Law enforcement and security organizations;
- (5) Maritime industry, including labor;
- (6) Other port stakeholders having a special competence in maritime security; and
- (7) Port stakeholders affected by security practices and policies.

In support of the Coast Guard's policy on gender and ethnic diversity, we encourage qualified women and members of minority groups to apply.

### Qualification of Members

Members must have at least 5 years of experience related to maritime or port security operations. Applicants may be required to pass an appropriate security background check before appointment to the Committee.

The term of office for each vacancy is 5 years. However, a member may serve one additional term of office. Members are not salaried or otherwise compensated for their service on the Committee.

### Format of Applications

Applications for membership may be in any format. However, because

members must demonstrate an interest in the security of the area covered by the committee, we particularly encourage the submission of information highlighting experience in maritime or security matters.

### Authority

Section 102 of the Maritime Transportation Security Act of 2002 (Public Law 107-295) (the Act) authorizes the Secretary of the Department in which the Coast Guard is operating to establish Area Maritime Security Committees for any port area of the United States. See 33 U.S.C. 1226; 46 U.S.C. 70112(a)(2); 33 CFR 1.05-1, 6.01; Department of Homeland Security Delegation No. 0170.1. The Act exempts Area Maritime Security Committees from the Federal Advisory Committee Act (FACA), Public Law 92-436, 86 Stat. 470, 5 U.S.C. App. 2.

Dated: December 7, 2006.

### Roy A. Nash,

*Captain, U.S. Coast Guard, Commander, Sector Southeastern New England.*

[FR Doc. E6-22424 Filed 12-28-06; 8:45 am]

**BILLING CODE 4910-15-P**

## DEPARTMENT OF HOMELAND SECURITY

### Coast Guard

[USCG-2006-26560]

### National Preparedness for Response Exercise Program

**AGENCY:** Coast Guard, DHS.

**ACTION:** Notice; request for public comment.

**SUMMARY:** The Coast Guard, the Pipeline and Hazardous Materials Safety Administration, the Environmental Protection Agency and the Minerals Management Service, in concert with representatives from various State governments, industry, environmental interest groups, and the general public, developed the National Preparedness for Response Exercise Program (PREP) Guidelines to reflect the consensus agreement of the entire oil spill response community. This notice announces the PREP triennial exercise cycle for 2007 through 2009, requests comments from the public, and requests industry participants to volunteer for scheduled PREP Area exercises.

**DATES:** Comments and related material must reach the Docket Management Facility on or before February 27, 2007.

**ADDRESSES:** You may submit comments identified by Coast Guard docket number USCG-2006-26560 to the

Docket Management Facility at the U.S. Department of Transportation. To avoid duplication, please use only one of the following methods:

- (1) Web Site: <http://dms.dot.gov>.
- (2) Mail: Docket Management Facility, U.S. Department of Transportation, 400 Seventh Street SW., Washington, DC 20590-0001.
- (3) Fax: 202-493-2251.
- (4) Delivery: Room PL-401 on the Plaza level of the Nassif Building, 400 Seventh Street SW., Washington, DC, between 9 a.m. and 5 p.m., Monday through Friday, except Federal holidays. The telephone number is 202-366-9329.

**FOR FURTHER INFORMATION CONTACT:** If you have questions on this notice, or need general information regarding the PREP or the triennial exercise schedule, contact Lieutenant Damon Sanders, Office of Contingency Exercises and Training (CG-3RPE), U.S. Coast Guard, telephone (202) 372-2151, or e-mail [Damon.C.Sanders@uscg.mil](mailto:Damon.C.Sanders@uscg.mil). If you have questions on viewing or submitting material to the docket, call Ms. Renee V. Wright, Program Manager, Docket Operations, telephone 202-493-0402.

### SUPPLEMENTARY INFORMATION:

#### Public Participation and Request for Comments

We encourage you to respond to this notice by submitting comments and related materials. All comments received will be posted, without change, to <http://dms.dot.gov> and will include any personal information you have provided. We have an agreement with the Department of Transportation (DOT) to use the Docket Management Facility. Please see DOT's "Privacy Act" paragraph below.

**Submitting comments:** If you submit a comment, please include your name and address, identify the docket number for this notice (USCG-2006-26560), indicate the specific section of this document to which each comment applies, and give the reason for each comment. You may submit your comments and material by electronic means, mail, fax, or delivery to the Docket Management Facility at the address under **ADDRESSES**; but please submit your comments and material by only one means. If you submit them by mail or delivery, submit them in an unbound format, no larger than 8½ by 11 inches, suitable for copying and electronic filing. If you submit them by mail and would like to know that they reached the Facility, please enclose a stamped, self-addressed postcard or envelope. We will consider all comments and material received during