U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-CIT
Phone: (202) 493-7678

COMDTINST 5230.62
MAY 29 2003

COMMANDANT INSTRUCTION 5230.62

Subj: USE AND MANAGEMENT OF COAST GUARD INTERNET AND INTRANET WEB SITES, CONTENT, AND ACCESS

Ref:
(a) E-Government Act of 2002, as amended
(b) United States Coast Guard Regulations, 1992, COMDTINST M5000.3 (series)
(c) Coast Guard Correspondence Manual, COMDTINST M5216.4 (series)
(d) Public Affairs Manual, COMDTINST M5728.2 (series)
(e) Paperwork Management Manual, COMDINST M5212.12 (series)
(f) Coast Guard Freedom of Information and Privacy Acts Manual, COMDTINST M5260.3 (series)
(g) Coast Guard Implementation of the Rehabilitation Act, Section 508, COMDTINST 5230.60 (series)
(h) Morale, Well-Being, and Recreation Manual, COMDTINST M1710.13 (series)
(i) Limited Personal Use of Government Office Equipment, COMDTINST 5375.1 (series)
(j) U.S. Coast Guard Heraldry, COMDTINST M5200.14 (series)
(k) Automated Information System (AIS) Security Manual, COMDTINST M5500.13 (series)

1. PURPOSE. This Instruction promulgates Coast Guard policy for use and management of the Coast Guard Internet and Intranet Web sites, content, and access. This includes command roles and responsibilities for Web content inherent in the chain of command.

2. ACTION. Area and district commanders, commanders of maintenance and logistics commands, commanders of field and headquarters units, assistant commandants for directorates, Chief Counsel, and special staff offices at Headquarters shall ensure compliance with this Instruction. Internet release authorized.

DISTRIBUTION – SDL No. 140

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	1	1	1		1	1	1	1	1	1		1	1	1	1	1	1	1	1		1					
B		8	10	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
C	1	1	1	1	1	1	1	1	1		2	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1
D	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1			1
E	1	1	1	1				1		1	1	1	1	1	1		1		1	1			1	1		
F																	1	1	1	1						
G	1	1	1	1	1																					
H																										

NON-STANDARD DISTRIBUTION:

3. DIRECTIVES AFFECTED. Policy on Coast Guard Use of Internet/Worldwide Web, COMDTINST 5230.56, and Coast Guard Intranet (CGWeb) Policy, COMDTINST 5230.57, are cancelled and superseded by this Instruction.

4. APPLICABILITY. The policies herein are applicable to all Coast Guard organizations and activities with the exception of the Coast Guard Exchange System (CGES). The Coast Guard Exchange System maintains its own IT Infrastructure and Internet presence with procedures approved by Commandant (G-WPX).

5. AUTHORITY AND RESPONSIBILITY.

   a. The Coast Guard Chief Information Officer (CIO), Commandant (G-CIT), shall:

      (1) Authorize all Coast Guard Web sites, Web servers, and domain names.
      (2) Designate an individual as the Web Program Manager for the Coast Guard.
      (3) Charter the Web Advisory Board (WAB).
      (4) Provide technical and procedural guidance for establishing and maintaining Coast Guard Web sites as necessary.
      (5) Establish and enforce Web policies and procedures in accordance with this Instruction.
      (6) Establish policy governing posting information to the Web.
      (7) Have the authority to establish Web style guides, templates, or other mechanisms to control the "look and feel" of Coast Guard Web sites and their content.
      (8) Establish a persistent Web site for providing procedural guidance to users and others responsible for Web management.
      (9) Have the authority to set standards and procedures for content posted to the Web.
      (10) Establish a single official location on the Intranet for all unclassified Commandant Directives, a single repository on the Internet for all Commandant Directives authorized for Internet release, and a management mechanism for keeping both repositories up to date with current official directives.
      (11) Establish Information System Security Plans (ISSPs) for the Coast Guard's Web infrastructure.
      (12) Establish and maintain the Coast Guard Electronic Reading Room in accordance with reference (a).

   b. The Coast Guard Web Advisory Board (WAB) is established by this Directive and shall:

      (1) Be comprised of members from a broad cross-section of Coast Guard operating organizations.
      (2) Provide vision and direction for implementation and use of the Web.
      (3) Be chaired by the Web Program Manager. An Executive Secretariat shall be designated to perform administrative duties related to WAB activities.
      (4) Broker and remediate concerns and conflicts related to use and management of the Web.
      (5) Have the authority to charter working groups comprised of selected members of the Coast Guard organization as necessary.

c. The Web Program Manager shall:

(1) Chair the WAB.
(2) Implement this Instruction and other guidance related to Web management.
(3) Advise the CIO on matters relating to management of the Web.

d. The Coast Guard Information Systems Security Program Manager, on the CIO's staff, shall:

(1) Provide policy guidance regarding information and information system security for the Web.
(2) Review and approve the Information System Security Plans (ISSPs) for Web systems.

e. Governmental and Public Affairs, Commandant (G-I), shall:

(1) Have final authority over content published to the Internet.
(2) Provide guidance on proper Internet and Intranet content.

f. Director of Command, Control, Communications, and Computers (Director of C4), Commandant (G-SC), shall, via the support infrastructure:

(1) Manage the Coast Guard's Internet and Intranet connectivity and ensure security of the Coast Guard data network.
(2) Conduct audits of Web content for operations security or information assurance violations, and advise the Web Program Manager of action to be taken.
(3) Protect Coast Guard systems from external intrusion/hacking, respond to computer security incidents, and advise the Web Program Manager of recommended future action.

g. All Commands hosting web servers shall:

(1) Provide access to Web content in accordance with this Instruction.
(2) Ensure that Coast Guard Web information and associated systems adhere to policies, laws, regulations, and guidance regarding security.
(3) Ensure security related system patches and upgrades are performed in a timely matter.
(4) Ensure proper security controls are in place to prevent unauthorized modification of information on web servers.

h. All commands maintaining a Web presence shall:

(1) Ensure that Web site initiatives within their respective areas of responsibility adhere to this Instruction and other laws, regulations, and guidance including those regarding accessibility, privacy, and security.
(2) Make every effort to minimize the use of bandwidth by their Web implementations.
(3) Establish a formal process for publishing information to the Web that accommodates the requirements of this Instruction and applicable references.

(4) Publish only that content which is rightfully within their purview.
(5) Designate a Web Content Manager. This designation conveys "by direction" authority to publish information on behalf of the Command as provided for in reference (b).
(6) Respond via the chain of command to periodic reporting, asset inventory, and certification requirements mandated by higher authority and announced by the CIO via official means.

i. Web Content Managers shall:

(1) Review and approve Web content within their area of responsibility.
(2) Manage Web content incidents within their area of responsibility.
(3) Ensure that Web content within their area of responsibility adheres to this Instruction and other policies, laws, regulations, and guidance including those regarding accessibility, privacy, and security.
(4) Provide guidance to Web Content Providers in accordance with authority delegated by the Unit Commander.

j. Web Content Providers shall:

(1) Develop Web content for publication.
(2) Adhere to policies, laws, regulations, and guidance including those regarding accessibility, privacy, and security.
(3) Adhere to guidance provided by the Web Content Manager.

k. Coast Guard employees shall:

(1) Comply with this and other directives prescribing use and management of Web information and associated systems.
(2) Report discrepancies or policy inconsistencies reflected in Web content to appropriate managers.

l. Coast Guard employees shall not:

(1) Access pornographic or other inappropriate material.
(2) Access streaming media for entertainment purposes.
(3) Access commercial Instant Messaging nor release sensitive CG information via commercial email.

6. DEFINITIONS.

a. *Content* refers to any kind of information published to the Web. This includes text, graphics, symbols, retrievable data, and presentation concepts.

b. *Internet* refers to the Coast Guard's publicly accessible Web presence available to all Internet users.

c. *Intranet* refers to the internally accessible Web presence and other domains available only to authorized users of Coast Guard owned networks. Non-Coast Guard persons and organizations such as contractors and other governmental or non-governmental agencies may have occasional or long-term authorized access to the Intranet for official business purposes.

d. *Extranet* refers to any private network that uses the Internet protocol and the public telecommunications system to securely share part of the Coast Guard's information or operations with suppliers, vendors, partners, customers, or other businesses. An extranet can be viewed as part of the Coast Guard's Intranet that is extended to users outside of the Intranet. An example is remote access used extensively in the Coast Guard. Though Extranets will not be discussed specifically in this Instruction, all policies that apply to Internet and Intranet apply equally to any Coast Guard Extranet.

e. *Special Use Application* refers to business software that uses the Web as all or part of its communications network. A Special Use Application generally has a limited audience and may have restricted access via user/password validation. The fact that a particular application may have a vast audience (for example, a human resources application accessible by all employees) does not exempt it from this category. Special Use Applications are not subject to this directive. Their development, including architecture, is approved as part of the Coast Guard's IT Capital Planning and Investment Control (CPIC) processes.

f. *The Web* refers generically to both the Internet and the Intranet, and by extension, any authorized Extranet implementation.

g. *Web Program Manager* refers to the official designated by the CIO to perform the normal duties of a Headquarters Program Manager for Web issues, which includes policy, budget, resource allocation, and high-level procedural guidance.

h. *Web Content Manager* refers to the individual designated by the Unit Commander to review and approve web content for the command and for commands under its administrative control. The duties of the Web Content Manager are inherently governmental. This individual is the command's primary point of contact for Web issues via the chain of command. This definition is provided as a means to commonly refer to this function and does not constitute the establishment of an official job description or billet requirement.

i. *Web content provider* refers to any individual who authors content for publication to Coast Guard Web sites. Web content providers must follow procedural guidance established by the command Web Content Manager under the authority of the unit commander. This definition is provided as a means to commonly refer to this function and does not constitute the establishment of an official job description or billet requirement.

j. *Web content incident* refers to situations where prohibited or inappropriate content is published to the Web. See paragraph 8.n for definition of prohibited content.

7. DISCUSSION.

   a. The Coast Guard Internet, Intranet, and Extranet are information and communications media critical to Coast Guard missions. It is imperative that these assets are managed in a manner that promotes efficiency, order, and accuracy, and avoids inappropriate usage.

   b. The Internet and Intranet have distinctly different purposes and users, managers, and Web content providers must thoroughly understand their primary distinctions.

   c. The Web is not a static medium. Design and technical management are subject to innovation and social change. A basic tenet of this Instruction is to explicitly state those policies that are lasting concepts not subject to such change.

   d. Other matters, such as content management requirements, use of specific technologies, and style guidelines are dictated in lower-level guidance promulgated by those given authority under this Instruction. The CIO will maintain up to date technical and policy guidance for Web Content Managers and content providers via a link from the CIO's home page on the Intranet.

8. POLICY.

   a. Web Content Management.

      (1) Web content management is a command function managed and supported via the chain of command.
      (2) Decisions regarding level of Web presence and level of support are made throughout the chain of command. All organizational components must balance the level of resources applied to their Web presence with some increased value in performing missions or other return on investment. This determination should be part of an overall strategy for optimal use of the Web and resources available to manage it.
      (3) All content on the Coast Guard Internet and Intranet is assumed to have been approved by the official having responsibility for the content within their respective administrative control. Every organizational component having a web presence within their respective administrative control is therefore responsible to ensure that their content, and that of their subordinate activities, conforms to this Instruction and any other guidance promulgated by the CIO and other cognizant authority.

   b. Web Content. Web content is official information published to the public and to internal Coast Guard users. It is subject to the same policies and guidance as normal correspondence or public affairs releases. It must therefore comply with references (c), (d), (e), and (f).

   c. Choice of Venue for Web Content. Since the Coast Guard's Internet and Intranet presences have two entirely different audiences, the choice of where to put information is important. The Intranet is intended for internal Coast Guard business, thus should be the primary location for

information intended to serve Coast Guard employees. The Internet presence is intended primarily for sharing information with the public or interacting with the external world. This does not mean that information intended for Coast Guard employees cannot be on the Internet, but if it is, security and privacy concerns must be dealt with carefully. If employee access from home is desired, one practical and secure solution is to use an Extranet approach, such as the approved remote access system.

d. Accessibility. All Internet and Intranet web pages shall comply with the provisions of reference (g). Web Content Managers shall ensure that persons with disabilities have access to Web services and information comparable to that of persons without disabilities. The Coast Guard CIO will publish supplemental implementation guidance, with references to helpful sources.

e. Links.

(1) Links from pages outside the Coast Guard are authorized in support of valid business objectives. Links may not endorse a particular non-Governmental product or service or provide preferential treatment. When selecting an external link, the user shall be presented with the following message:

"Links from these pages (or "this page" on a specific page of links) to non-Coast Guard sites are provided as a customer service and do not represent any implicit or explicit endorsement by the United States Coast Guard of any commercial or private issues or products presented there."

(2) Links on Internet sites to Intranet sites are specifically prohibited, since security provisions to protect the Coast Guard data network would render these links "broken." Links embedded in documents posted to the Internet are exempted but should be avoided if practicable.

(4) No payment of any kind shall be accepted to provide a link on any Coast Guard Web page to another web page or to provide specific content on a Coast Guard web page.

f. Hosting Services. All Coast Guard Internet web sites shall be hosted on a Coast Guard or Department of Homeland Security (DHS) Internet web server unless an alternative ".gov" or ".mil" domain is approved by the CIO. All Coast Guard Intranet web sites shall be hosted on CIO approved Coast Guard Intranet servers. This excludes Web-based special use applications (see definition in paragraph 6.e.) which have been approved to be hosted on a separate servers via the IT Capital Planning and Investment Control (CPIC) processes. Requests to host on other servers, use other primary domains, or implement an Extranet must be approved by the CIO. Waiver requests shall be submitted to the WAB. A compelling justification will be required and security concerns will be paramount. If approved, the Telecommunications and Information Systems Command (TISCOM), under the direction of the Director of C4, will process the appropriate Domain Name Server (DNS) change requests.

g. Information Dissemination. All organizational components publishing information to the Web shall ensure that the content posted is within their purview and that they have authority to publish it. This constitutes release of information to the public, which is governed by the policies

provided in references (d) and (f). Links to the official location of Commandant Directives and external agency documents are allowed; posting those documents on organizational websites is prohibited for two reasons. First, they can become out of date without the user being aware, and second, they consume Coast Guard system resources.

h. Information Gathering. All Coast Guard Internet web sites shall comply with the Coast Guard's published privacy policy (linked to the Coast Guard Internet "Home" page). Any use of the Internet to gather information on the public must be approved by the DHS CIO, via the Coast Guard CIO. Examples of information gathering techniques include:

(1) Implementing user registration schemes.
(2) Using persistent cookies for data collection.
(3) Maintaining lists of visitor email addresses.

i. Non-Appropriated Fund Activities (NAFA).

(1) Commercial sponsorships, advertisements and endorsements are prohibited on publicly accessible pages of official Coast Guard web sites (".mil"). Web sites are official communications to the public. Just as the Coast Guard would not print advertisements on news releases, commands shall not post advertisements on publicly accessible official Coast Guard web sites. Additionally, commands shall ensure that the credibility of official information is not adversely affected by association with commercial sponsorships, advertisements or endorsements.

(2) In accordance with the policies contained in Reference (h), commands may develop non-appropriated fund web sites (".com"), may have commercial sponsorships, and may sell electronic advertising. Advertisements on these web sites are intended for eligible patrons of the MWR program, as defined in reference (h). As noted in reference (h), advertising or sponsorship cannot directly or indirectly compete with the Coast Guard Exchange System.

(3) Commands are encouraged to include official information about non-appropriated fund activities on official Coast Guard web sites as long as the information does not include commercial sponsorships or advertisements.

(4) With command approval, NAF activities may use non-appropriated funds to develop and maintain commercial web sites for unofficial information, where commercial sponsorship or advertising may appear. External links to authorized, unofficial NAF commercial web sites are authorized, with an appropriate disclaimer preceding the actual connection to the NAF commercial web site to avoid product endorsement or preferential treatment. Official information pertaining to the NAF activity may be posted on the commercial non-appropriated fund web site with command approval, but only if it is also posted on the official publicly accessible Coast Guard web site. Other official information shall not be posted to the commercial site

j. Official Descriptions of Missions and Entities. Publish only official descriptions of Coast Guard missions and entities.

k. Official Records. Wherever official records are disseminated via the Web, procedures shall be established to ensure that the records have been carefully reviewed and comply with all applicable policies and procedures pertaining to records management per reference (e). Every effort shall be made to ensure these records cannot be altered by unintended audiences.

l. Privacy. Coast Guard personnel do not have a right, nor should they have an expectation of, privacy while using the Web when accessed via Government computers or networks. All Intranet and Internet activities are subject to monitoring at all times.

m. Personal Use. Generally, Coast Guard Web access via Coast Guard owned networks is provided for official use only. Limited personal use of Government office equipment is governed by reference (i), which describes the scope of limited personal use and specifically prohibited usage as it relates to the Web.

n. Prohibited Content. The following categories of information and content shall not be published to any Coast Guard Web site or page except as noted by "*:"

(1) Copyrighted or trademarked material without explicit permission from the author.
(2) Classified information.
(3) For Official Use Only (FOUO) information. *
(4) Inflammatory comments.
(5) Political statements.
(6) Pornographic material.
(7) Information protected under the Privacy Act in accordance with reference (f).
(8) Information regarding Coast Guard personnel.* Names and duty addresses of personnel assigned to units that are sensitive, routinely deployable, or stationed in foreign territories shall not be released nor shall such individuals be identified in photographs or articles.
(9) Information on family members of Coast Guard personnel, except necessary contact information for those serving in an official capacity, such as Command Ombudsman.
(10) Information which would interfere with an official investigation or Law Enforcement (LE) activity, or judicial proceeding, including information which could subject LE personnel to potential harm.
(11) Internal program agenda, correspondence, and memos not appropriate for general distribution. *
(12) Personal opinion or private agenda unless the information is clearly unofficial such as in a discussion forum.
(13) Duplication of Commandant Directives or other Government documents (one official copy of Commandant Directives is published on the Web by the CIO; other organizations shall link to those and external documents published by other Government agencies, rather than including them on their own websites).
(14) Pre-decisional information, reader files, internal letters and memoranda shall not be released unless approved by the appropriate authority. *

(15) Links from Coast Guard Internet sites to Coast Guard Intranet sites. Links within documents or that occur at happenstance are allowed - the intent is to avoid a "broken" link where the reader may have an expectation to view the content.
(16) Procurement-sensitive or proprietary information. *
(17) USCG Seal (with gold braid), in accordance with reference (j).
(18) Operations Security (OPSEC) and Information Assurance material. *
(19) Advertisements or endorsement of commercial products or services.
(20) Online sale of merchandise.

* May be posted on Intranet only if sufficient access controls are in place, such as user name, passwords, or other technical controls (e.g. encryption), or if the content is deemed suitable for all Intranet users. TISCOM, operating under the authority of Commandant (G-SCT), will provide guidance.

o. References to the Coast Guard. All initial references to the service on the Internet shall use either the form "United States Coast Guard" or "U.S. Coast Guard."

p. Security and Access Controls. Web servers and their supporting network infrastructure are official systems as defined by reference (k), thus all security provisions in that directive apply, including the requirements for:

(1) Security risk assessments.
(2) Information System Security Plan (ISSP).
(3) AIS System Security Certification and Accreditation.

q. Use of Internet Resources.

(1) Coast Guard Web sites and pages shall be established only for official, mission-related or mission supporting purposes except as provided for below.
(2) In accordance with reference (i), limited incidental personal use is authorized in accordance with Government-wide policies on personal use of Government property and office equipment.
(3) Coast Guard Web servers shall not be used to host or store web sites or pages not authorized by the CIO.
(4) All activities sponsoring Web pages shall give due consideration and make every effort to minimize the use of bandwidth by their Web implementations.

r. User Feedback. Managers of sites or pages that provide the ability to contact the Coast Guard with the expectation of a response shall ensure that a mechanism is in place to provide an accurate response to legitimate requests within a reasonable timeframe - see reference (e). Managers should consider that a highly publicized event may produce an avalanche of information requests from the public, and that such requests may have significant Public Affairs implications. See reference (d). And note that reference (f) contains specific policy on response to Freedom of Information Act (FOIA) requests submitted by electronic mail.

9. WEB BASED APPLICATIONS AND INNOVATIONS.

   a. As in any area of Information Technology, innovation is encouraged and highly valued. Historically, the majority of innovative initiatives have originated in the field, not Headquarters, but local solutions sometimes conflict with Enterprise strategies.

   b. What may be an easy and inexpensive innovation locally may be far more costly to implement at the Enterprise level. The Enterprise view must consider the issues mandated by the Coast Guard IT Capital Planning and Investment Control (CPIC) processes, including long-term support, training, security, cost, and management issues that are easy to overlook in a local initiative.

   c. The CPIC process has monetary thresholds and compliance issues not present in local innovation, and which often get triggered when Programs or the Innovation Council attempt to capitalize upon a local initiative and deliver it to the Enterprise. In particular, local initiatives seldom have to consider the incremental cost of Government staff time, where an Enterprise system may have to seek budgetary support for staff or contractor support to sustain it.

   d. In cases where an innovation (or its basic concept) is adopted Enterprise-wide, local Commanders may have to abandon their local initiative and adopt the Enterprise solution. One benefit to the local Commander is that this frees up resources with which to pursue further innovation, although it has the appearance of an unjust reward for their innovative initiative.

10. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental aspect and impact considerations were examined in this Directive and have been determined to not be applicable.

11. FORMS/REPORTS. None.

T. W. ALLEN/s/
Chief of Staff