



DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

SECNAVINST 5720.47A
CHINFO
October 24, 2003

SECNAV INSTRUCTION 5720.47A

From: Secretary of the Navy
To: All Ships and Stations

Subj: DEPARTMENT OF THE NAVY POLICY FOR CONTENT OF PUBLICLY
ACCESSIBLE WORLD WIDE WEB SITES

Ref: (a) DoD Policy Memorandum Web Site Administration,
Dec 7, 98 with updates
(b) SECNAVINST 5720.44A, Department of the Navy Public
Affairs Policy and Regulations
(c) SECNAVINST 5430.97, Assignment of Public Affairs
Responsibilities in the Department of the Navy
(d) CNO WASHINGTON DC 261622Z MAR 99 (NAVADMIN 088/99)
(e) SECNAVINST 5211.5D, Department of the Navy Privacy
Act (PA) Program
(f) SECNAVINST 5720.42F, Department of the Navy Freedom
of Information Act (FOIA) Program
(g) SECNAVINST 5510.36, Department of the Navy (DON)
Information Security Program Regulation
(h) SECNAVINST 5239.3 Department of the Navy
Information Security (INFOSEC) Program
(i) DoD Directive 5040.5 Alteration of Official DoD
Imagery, Aug 29, 95
(j) 29 U.S.C. 794d (Section 508 of the Rehabilitation
Act) (NOTAL)
(k) 44 U.S.C. 3501 (Paperwork Reduction Act)
(l) OMB Circular A-130 (Management of Federal Information
Resources)

Encl: (1) DON Web Site Administration Definitions
(2) DON Publicly Accessible Web Site Policy and
Procedures

1. Purpose. To implement reference (a) within the Department of the Navy (DON) and provide additional policies and procedures governing the content of Department of the Navy publicly accessible World Wide Web (WWW) sites.

2. Cancellation. SECNAVINST 5720.47 and ALNAV 58/02, Removal of Personally Identifying Information of Department of Defense (DoD) Personnel from Unclassified Web Sites.

3. Scope. This instruction is applicable throughout the DON. It applies to all DON activities and all publicly accessible DON Web sites designed, developed, procured, or managed by DON activities and/or by their contractors.

4. Background

a. The WWW is an extremely powerful public information tool, and its use, within these guidelines, is encouraged. This instruction assigns responsibilities and prescribes policies implementing reference (a) within the DON, to ensure appropriate use of the Web to provide public information to a global audience.

b. The management, including oversight, of all content on a publicly accessible Web site is a public affairs function.

c. The development of Web technology and the ease with which information can be posted to the Web has given rise to the proliferation of command Web sites. The Web was, and is specifically designed to be, open and accessible to a global audience. While this global accessibility makes the Web a powerful public information tool and a productivity enhancer in the conduct of daily business, it also presents a risk to DON personnel, assets and operations if inappropriate information is published on command Web sites. The global reach of the WWW requires special precautions be taken when posting information to this medium. Millions of Web users around the world can easily gain access to DON public Web sites, rapidly collect information, add it to information already collected from other public sites, and assemble it in a way that is not possible through any other media. Computer software and Internet-based search engines have given Web users the ability to automatically "mine" data and collect an aggregate of information that can pose a threat to the security of Navy and Marine Corps operations and the safety of DON personnel and their families. Additionally, worldwide terrorists may target DON personnel, and foreign intelligence operations may specifically target those individuals involved in Navy research and development. More than ever, the need to provide public information to the Navy's and Marine Corps' various audiences must be balanced with the need to protect operational security, privacy of information, and personal safety.

d. As the WWW proves itself to be a cost-effective method of moving information and as DON becomes increasingly dependent on the Internet, any sustained attack on the Internet could have

serious ramifications for naval operations. In a number of computer network attacks, the attack is often preceded by gleaning information about a command from its publicly accessible Web site and combining it with other publicly accessible information. Additionally, this information may be used by an adversary to disrupt DON operations or target individuals. By its very nature, the WWW greatly facilitates information collection and aggregation.

e. The appearance, accuracy, currency and relevance of the information presented by Navy and Marine Corps commands on their Web sites reflects on the DON's professional standards and credibility. Additionally, information residing on a Web server associated with a "navy.mil" or "usmc.mil" domain is interpreted by the worldwide public, including the American taxpayer and media, as reflecting official Navy or Marine Corps policies or positions. Therefore, all information presented must be accurate and current.

f. The benefits of using the WWW as a public information tool must be balanced with security and safety concerns. Commanders must strike a balance between openness in government (easy access to DON information) and the need to safeguard information which, if released to the general, global public, could adversely affect the national interest, the conduct of DON operations and programs, or place DON commands, personnel or their families at risk. Potential risks must be judged and weighed against potential benefits prior to posting any DON information to the WWW.

5. Definitions. Terms used in this instruction are defined in reference (a) and further in enclosure (1).

6. Policy. Reference (a) provides primary governing policy for all unclassified DoD WWW sites. Detailed policy on administration of publicly accessible WWW sites, in amplification of reference (a), is provided in enclosure (2).

7. Action

a. The DON Chief Information Officer (DONCIO) is responsible for providing Department-wide information management and information technology (IM/IT) policy and guidance.

b. The DON Chief of Information (CHINFO) is responsible for the development and administration of DON public affairs policies and procedures per reference (b). The U.S. Marine Corps Director of Public Affairs (DIRPA) is responsible for implementation of DON public affairs policy and the development and administration

of USMC public affairs policies and procedures per reference (c). Additionally, CHINFO and DIRPA each will:

(1) CHINFO will maintain a master WWW page displaying DON Web policy for publicly accessible WWW sites on the Navy's official Web site and DIRPA will link to that page. All significant changes to this Web page and/or its location will be issued via naval (ALNAV) message.

(2) Administer and maintain the official U.S. Navy Web site at www.navy.mil or the official U.S. Marine Corps Web site at www.usmc.mil for the posting of appropriate U.S. Navy- or Marine Corps-level information and images.

(3) Maintain overall cognizance for U.S. Navy Web sites or U.S. Marine Corps Web sites content-related questions as they pertain to the appropriateness of publicly accessible material. This responsibility includes cognizance regarding Privacy Act (PA), Freedom of Information Act (FOIA) and public affairs material but will not include issues related to the security of operations or classified information.

(a) For Navy PA/FOIA issues, CHINFO will coordinate, as appropriate, with Head, DON PA/FOIA Policy Branch [CNO (N09B-10)].

(b) For Marine PA/FOIA issues, DIRPA will coordinate, as appropriate, with the Counsel to the Commandant, the Marine Corps Inspector General (IG), the Staff Judge Advocate (SJA) to CMC (JAR), and/or the Headquarters, Administrative Resources Branch (ARSE).

(c) CNO (N6/N7) is responsible for issues related to security of operations and classified information for the Navy. The Director, Command, Control, Communications and Computers (C4) is responsible for issues related to security of operations and classified information for the Marine Corps.

c. Commander Naval Network Warfare Command (NETWARCOM) and Commander, United States Marine Corps Network Operations and Security Command (MCNOSC) are responsible for establishing procedures to ensure operational integrity and security of the computers and networks supporting DON Web sites. Additionally, NETWARCOM and MCNOSC each will:

(1) Conduct assessments of U.S. Navy or U.S. Marine Corps Web sites at least annually as required by Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C3I)) to ensure compliance with information assurance and security policy requirements.

(2) Notify the responsible Echelon 2 commander when a site is discovered to be non-compliant to ensure the site is either removed from the WWW or brought into compliance.

(3) Maintain overall cognizance for questions about U.S. Navy or U.S. Marine Corps Web sites as they pertain to the security of computer operations or classified information.

(4) Establish and maintain a central Web site registration system for all U.S. Navy commands in accordance with reference (a). A Marine Corps Web site registration system will be established by DIRPA and coordinated with C4 for Corps-wide compliance and review.

(5) Establish a mechanism for receiving and reviewing all requests for U.S. Navy or U.S. Marine Corps waivers to provisions of this policy relating to security of computer operations. Waivers will be considered based on provisions of current law and directives. Requests for waivers will be submitted via the chain of command.

d. DON commands and activities that maintain publicly accessible Web sites will implement and administer a comprehensive Web site management program under this instruction. In accordance with reference (b), information posted on a command/activity publicly accessible Web site must be approved for release by the command/activity release authority. Each addressee who maintains a publicly accessible WWW site as defined in this instruction shall:

(1) Ensure all information currently residing on the command/activity Web site is accurate, and is appropriate for viewing by a worldwide audience, friend and foe alike. Information not suitable for a publicly accessible Web site must either be removed or placed on a restricted-access site. Per ASD (C3I) guidance, domain restriction alone is not sufficient.

(2) Develop local procedures for the approval of information posted on command/activity publicly accessible Web sites. At a minimum, this process shall include review to ensure posted information meets requirements set forth in references (a) through (1) and this instruction.

(3) Designate, in writing, a primary Web site manager, who may be known as the webmaster. Information on how to contact the web manager (e.g., email address) will be included in the command's "home page" source code. At a minimum, the web manager shall:

(a) Maintain a library of current applicable instructions, notices, ALNAVs, and NAVADMINS regulating content of DON publicly accessible Web sites and shall be conversant in the provisions of these directives.

(b) Serve as principal point of contact on all matters pertaining to administration of the publicly accessible Web site.

(c) Oversee the command's Web site and ensure compliance with current directives. Oversight includes monitoring the site as often as possible to ensure no unauthorized changes have occurred.

(d) Register the site with the Fleet Information Warfare Center's (FIWC) Navy Web Site Registration System (NWSRS). The NWSRS can be accessed through, and is integrated with, Government Information Locator Service (GILS). Registration with NWSRS will automatically register the site with GILS as required by Public Law 104-13. Commands will review and update their registration on a yearly basis or whenever there is a change in any of the registration data fields.

(e) Provide training for activity/command personnel on the provisions of reference (a) and this instruction.

e. Compliance with this instruction will be made part of the command inspection program at each level within the chain of command. Audits of the web sites of subordinate commands will be made annually.

Gordon R. England

Distribution:

SNDL, Parts 1 and 2

MARCORPS Codes 71000000000 and 71000000100

DEPARTMENT OF THE NAVY WEB SITE ADMINISTRATION

DEFINITIONS

1. Internet - A network of networks - a world-wide public network that links many smaller networks. Having access to the Internet means being able to send and receive e-mail, partake in interactive conferences, access information resources and network news, and transfer files.
2. World Wide Web (WWW) - A part of the Internet displaying text and pictures through the use of computer software called a browser. The WWW originated at the European Laboratory for Particle Physics (CERN) in Geneva, Switzerland. Unless operating behind a userid/password or domain filtering scheme, WWW sites are accessible to anyone in the world who has a computer and connectivity via an Internet Service Provider (ISP).
3. Intranet - A network based on TCP/IP protocols (as with an internet) belonging to an organization, accessible only by the organization's members, employees, or others with authorization. The firewall surrounding an intranet can be used to prohibit unauthorized access. By definition, intranet sites are not publicly accessible, and therefore are not covered by this instruction.
4. Extranet - An intranet that is partially accessible to authorized outsiders. Whereas an intranet resides behind a firewall and is accessible only to people who are members of the same organization, an extranet provides various levels of accessibility to outsiders. One can access an extranet only if one has a valid username and password, and your identity determines which parts of the extranet you can view. Web-based communication occurring behind a security scheme (i.e. behind a userid/password or domain/IP filtering scheme), often referred to as an "extranet," is, for the purposes of this instruction, considered a virtual intranet, and not accessible to the public, and therefore not covered by this instruction.
5. Web Site - A Web site describes an entity and its services, and consists of a single page or a collection of related, and linked, pages. All content presented on DON Web pages is considered to be official. All Web sites/pages created by DON employees and/or contractors and containing information about the command/activity or part thereof are considered as official DON Web sites/pages. A publicly accessible Web site is one on which there are no restrictions to access.

6. Web Page - A single document existing within the Web site, a Web page might be an HTML document, an image, a .PDF document, PPT document, XLS, etc.

7. Home Page - The logical starting (entry) point of a World Wide Web (WWW) site. It is similar to the title page and table of contents of a printed document. A home page usually contains links to subsequent pages within the site. While the home page is the most common access point to a site, it is not the only access point. Any WWW document can be accessed directly from a link or by using its Uniform Resource Locator (URL) address.

8. Domain - A part of the Domain Name System. The domain to the farthest right is called the top-level domain. The top level domain in "www.navy.mil" is ".mil" which is reserved for U.S. military. The second-level domain for the U.S. Navy is "navy.mil" and the second-level domain for the U.S. Marine Corps is "usmc.mil". Other top-level domains include ".edu", ".gov", and ".com".

9. Web Manager - A person who maintains a Web page, Web site, and/or the server upon which the Web site resides. May also be referred to as a "webmaster."

10. .HTM, .HTML - the extension for Web documents written in Hypertext Markup Language (HTML) which is the format (code) in which Web pages are written. The extension "signals" the browser (reading software) what type of file to decode and display.

11. Source Code - The HTML coding which tags and formats the information to make it viewable by the browser. The source code itself is not normally viewed by the browser.

12. URL - Uniform Resource Locator. An Internet "address" of a resource. URLs can refer to Web pages, file transfer protocol (FTP) sites or files, Gopher resources, or NNTP (Usenet) Newsgroups.

13. HTTP - HyperText Transfer Protocol is the method by which WWW HTML pages are transferred (served) from the Internet to the local computer's Web browser and then displayed.

14. Link - A connection from one Web document or file to another, not necessarily within the same Web site. The link typically appears as a word, or phrase, often with blue, underlined letters (hypertext). As the cursor touches the link, the cursor takes the form of a hand. Clicking the mouse button causes the Web browser to connect to the document pointed to by the link.

15. Web Browser - Software that allows a user to retrieve information from Web servers.

16. Web Server - A software/hardware suite, that responds to content queries from Web Browsers with the content requested. This content is retrieved from its own store of hosted web sites.

DEPARTMENT OF THE NAVY WEB SITE ADMINISTRATION
PUBLICLY ACCESSIBLE WEB SITE POLICY & PROCEDURES

1. Authority. The establishment of a command Web site on the publicly accessible WWW remains a command prerogative, consistent with other leadership responsibilities for public communication.

a. All DON Web sites must have a clearly articulated purpose, approved by the commander, and supporting the command's/activity's core competency mission.

b. Web sites published by or under the aegis of Navy/Marine Corps commands but hosted on commercial servers (servers with other than "usmc.mil" and "navy.mil" top level domains) are also considered official sites and remain subject to this instruction and reference (a).

c. Publicly accessible Web sites are limited to the command level, i.e. - to that organization with one or more Unit Identification Codes. No separate Web sites will be established for any entity below the command (or command equivalent) level. As example, but not all-inclusive, there shall be no departmental or divisional Web sites external to the command's Web site. These departmental/divisional/office pages will reside within the command's Web site. An example URL would be www.commandname.navy.mil with departmental/divisional/office page(s) names following the top level domain (i.e. - www.commandname.navy.mil/officename/). DON-wide special programs (i.e. FOIA, Privacy Act, and others) are exempted from this requirement and may be stand-alone Web sites (i.e. - www.specialprogram.navy.mil). Approval for these special program Web sites must be submitted via the chain of command to the Chief of Information (ATTN: OI-6).

d. A designation of "Unofficial" is not recognized for Navy Web sites. Any Web site created by any entity of the Navy including those done under any contract or agreement for any entity of the DON constitutes an official Web site and is subject to this instruction. Web sites about the Navy created by persons not actively connected to the DON and containing information not provided by any entity of the DON are considered personal Web sites. Those persons may include the general public, retirees, family members, and service members or DON employees when the information posted is clearly not information available because the individual is a service member or DON employee.

2. Administration

a. All DON Web sites must be protected from modification on systems exposed to public networks in accordance with references (f) and (g).

b. All command/activity home pages -- the logical entry point of the command/activity Web site -- must contain, at a minimum, the following:

(1) Full organizational name and official postal mailing address.

(2) A statement that the site is an official U.S. Navy or U.S. Marine Corps Web site.

(3) A prominently displayed hypertext link to a tailored Privacy and Security Notice on the home page. All references to the Privacy and Security Notice shall state: "Please read our Privacy and Security notice." Overt warning signs or other graphics such as the "skull and crossbones" or "cloak and dagger," or wording indicating danger or warning are specifically forbidden. The tailored Privacy and Security Notice will be based on the following:

Notice: This is a U.S. Government Web Site

This is a World Wide Web site for official information about [the name of command/activity]. It is provided as a public service by [command/activity name and servicing command if applicable]. The purpose is to provide information and news about the [name of command/activity] to the general public. All information on this site is public domain and may be distributed or copied unless otherwise specified. Use of appropriate byline/photo/image credits is requested. Unauthorized attempts to upload information or change information on this Web site are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

Except for authorized law enforcement investigation and to maintain required correspondence files, no other attempts are made to identify individual users or their usage habits. Raw data logs are used to simply determine how many users are*

accessing the site, which pages are the most popular, and, from time to time, from which top level domain users are coming. This data is scheduled for regular destruction in accordance with National Archives and Records Administration guidelines.

The following, when appropriately tailored, may be used as a notice for sites using session cookies.

Cookie Disclaimer. *[name of command/activity] does not use persistent cookies, i.e., tokens that pass information back and forth from your machine to the server and remain after you close your browser.*

[name of command/activity] does use session cookies, i.e., tokens that remain active only until you close your browser, in order to (make the site easier for you to use). No database of information obtained from these cookies is kept and when you close your browser, the cookie is deleted from your computer.

[name of command/activity] uses cookies in the following ways:

(Describe use, e.g., "to save you time in filling out forms," "to maintain a relationship between the image and the correct link, the program that displays the banners on the bottom of some of our pages uses a session cookie.")

You can chose not to accept these cookies and still use the site, but (you may need to enter the same information repeatedly and clicking on the banners will not take you to the correct page). The help information in your browser software should provide you with instruction on how to disable cookies.

* The words "Raw data logs" must be hyperlinked to a Web page containing the following information:

NOTE: The information below should be tailored, if necessary, to show an accurate example of the specific information being collected.

Example: Information Collected from [name of command/activity] for Statistical Purposes

Below is an example of the information collected based on a standard request for a World Wide Web document:

136.205.11.176 - - [18/Jun/2001:11:24:03 -0500] "GET /navpalib/ships/carriers/ HTTP/1.1" 200 2575
136.205.11.176 - this is the host name (or IP address) associated with the requester (you as the visitor). In this case, the requester is coming from a Navy address. Depending on the requester's method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet Service Providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address.

[18/Jun/2001:11:24:03 -0500] -- this is the date and time of the request

/navpalib/ships/carriers/ HTTP/1.1 -- this is the location of the requested file on the Navy's Web site.
200 -- this is the status code - 200 is OK - the request was filled

2575 -- this is the size of the requested file in bytes

Mozilla 3.0 -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages
www.altavista.digital.com - this indicates the last site the person visited, which indicates how people find the Navy's Web site.

A notice for use on non-publicly accessible Web sites is contained in reference (a).

c. In accordance with reference (j), all DON Web publicly accessible Web sites will provide accessibility to all U.S. citizens, including persons with disabilities. This is not intended to permit open public access to those sites behind any security scheme, but those sites must be accessible to authorized persons who also might have disabilities.

d. Command Web sites shall contain links to the following sites:

(1) The Navy's official Web site at <http://www.navy.mil> and/or the Marine Corps' official Web site at <http://www.usmc.mil>.

(2) The parent command, or Immediate Superior In Command (ISIC), home page where applicable.

(3) The Navy and/or Marine Corps recruiting sites at <http://www.navy.com> and <http://www.marines.com>.

(4) The Navy's official Freedom of Information site at <http://foia.navy.mil/>

3. Content

a. All information, graphics and photos posted on publicly accessible DON Web Sites must be carefully reviewed to ensure they meet the standards and requirements as published here, including operational security (OPSEC) considerations.

b. Photography

(1) Photos may not be altered in any way. Standard photographic practices of cropping, sizing, dodging, or burning are not considered alteration. Reference (h) applies.

(2) All photos posted to any command Web site will also be provided to the Navy Office of Information, Visual News Service, at navyvisualnews@navy.mil. The Visual News Service is the official release authority to the international and national media.

c. In addition to requirements of reference (a), all DON Web sites shall:

(1) be presented in a manner reflecting the professionalism of the DON;

(2) comply with the Privacy and Freedom of Information Acts, references (d) and (e).

(3) contain only "approved for release" general information suitable for viewing by anyone any place in the world, friend and foe alike.

(4) contain only those images which support the overall mission of the Web site. Images with captioning will only have caption information suitable for viewing by worldwide audience, both internal and external. Images of personnel will not contain personal information for individuals other than name, rank/rate, and duty station.

(5) be current, accurate and factual, and reflect only information for which the publishing command has release authority.

d. Specific Web site restrictions include:

(1) Web sites will not include classified material, "For Official Use Only" information, proprietary information, or information that could enable the recipient to infer this type of information. This includes, but is not limited to, lessons learned or maps with specific locations of sensitive units, ship battle orders, threat condition profiles, etc., activities or information relating to ongoing criminal investigations into terrorist acts, force protection levels, specific force protection measures being taken or number of personnel involved, Plans of the Day, or Plans of the Month. When it is necessary to gain release authority from a senior in the chain of command, subordinate commands will submit material for clearance only after it has been reviewed and necessary amendments made to the fullest capability of the submitting command.

(2) Web sites will not identify family members of DON personnel in any way, including in photos or photo captions, except for the spouses of senior leadership who are participating in public events such as ship namings, commissionings, etc., nor will family member information be included in any biographies.

(3) Web sites must not include information for specialized, internal audiences. Familygrams, internal news service products and other information may be posted if they are general, suitable for an external audience, and comply with content restrictions of this instruction. Access to information that is intended for a specialized internal audience should be restricted using DOD-approved access control mechanisms.

(4) Web sites must not contain any written information or display any logo indicating the Web site is best viewed with any specific Web browser(s); or, that the Web site has been selected as a recommended or featured site by any organization, or, point to any particular search engines or recommend any commercial software. Web sites developed and/or maintained by contractors may not include the contractor's name nor may they link to the contractor's Web site.

(a) Web sites will not provide commercial software, or links to commercial software except in those cases where the software is unique and required for viewing documents provided within the Web site's purpose. An example is Adobe Acrobat required to read Portable Document Files (.PDF) used for viewing documents which must be presented in an unalterable form. In these cases, only a text link directly to the vendors download web page is permitted. There will be no use of corporate logos.

(5) Web sites will not display any logos or graphics for events, issues, or commemorations unless that event, issue, or commemoration is command-sponsored (i.e., a command event), or is approved by the Secretary of the Navy if that event, issue, or commemoration is national in scope. Examples, but not all inclusive, of approved events, issues, or commemorations that are national in scope are Navy Birthday, POW/MIA Day, and Federal secular holidays.

(6) Web sites shall not contain any material that is copyrighted or under trademark without the permission of the copyright or trademark holder. Further, the material must relate directly to the command's primary mission. Works prepared by DON personnel as part of their official duties and posted to the command Web site may not be copyrighted, nor may the Web site itself be copyrighted.

(7) Web sites shall not display personnel lists, "roster boards," organizational charts, or command staff directories which show individuals' names, individuals' phone numbers or e-mail addresses which contain the individual's name.

(a) General telephone numbers and non-personalized e-mail addresses for commonly-requested resources, services, and contacts, without individuals' names, are acceptable.

(b) The names, telephone numbers and personalized, official e-mail addresses of command/activity public affairs personnel and/or those designated by the commander as command spokespersons may be included in otherwise non-personalized directories, etc.

(c) If deemed by the commander as a best business practice, the Navy Personnel Command may post names and official e-mail addresses of detailers. Naval Medical Centers and Naval Hospitals may also post names and official e-mail addresses of primary care providers and Patient Affairs representatives.

(d) Given that the academic environment has professional requirements for maintenance of academic standing, the professional academic staff of Navy institutions of higher education (the Naval Academy, Naval Postgraduate School, and Naval War College), but not the support staff, may be identified by name, specialty, etc., as required to maintain academic standing. Additionally it is apparent that, in an academic institution, the faculty by reputation/academic standing or by nature of their positions may interact with the public as part of the process of recruiting students, and thus some identifying information is appropriate. However, such information should

include only professional information, not information on their families, place of birth, hobbies, etc., not related to their academic credentials.

1. Photos will remain restricted to the institutions senior leadership and will not extend to department heads nor faculty.

2. For support staff and other departments, contact information will only be generic, e.g., Admissions Office, phone XXXX, e-mail: Admissions@command.navy.mil and contain no personal information.

(8) Biographies. The biographies of flag officers, commanders, commanding officers, officers in command, executive officers or deputies, the civilian equivalents of those officers just listed, and command master chief petty officers or Marine Corps master gunnery sergeants or sergeants major may be posted to command/activity Web sites. However, biographies published on publicly accessible Web sites will not include date of birth, current residential location, nor any information regarding family members.

(a) Naval Medical Centers and Naval Hospitals may also post names, portraits and official e-mail addresses of primary care managers, i.e., those who see patients. In each case, the portraits, head and shoulders, may not be larger than 200 pixels in width.

(b) Because of the unique community relations nature of the mission of the U.S. Navy Flight Demonstration Squadron, of the U.S. Navy Band and its component units, and Fleet bands, portraits and biographies of command/unit members are permitted, providing such biographies are in compliance with other sections of this instruction. In each case, the portraits, head and shoulders, may not be larger than 200 pixels in width.

(9) Links. In order to avoid the appearance of official endorsement, Web sites will not link to non-government, commercial-entity sites except as follows:

(a) The U.S. Navy and U.S. Marine Corps official Web sites (<http://www.navy.mil> and <http://www.usmc.mil>) may link to Federally-chartered, military-related organizations. Commands desiring to link to military-related organizations' Web sites will do so only by linking to the appropriate pages on the U.S. Navy or U.S. Marine Corps official Web sites.

(b) Links to appropriate private sector non-commercial sites by the Bureau of Medicine or by the Chief of

Chaplains may be made for purposes of additional educational resources, provided those links support the command's core mission and avoid the appearance of official endorsement.

(c) As part of the command's family support function, Web sites of bases, air stations, or equivalent commands may link to local Chambers of Commerce (or overseas equivalents) and local government agencies. Tenant commands will link to the base Web site to provide access to these external links. Links made to provide weather services may be made only to the appropriate Navy Meteorology and Oceanography Center or to the National Weather Service of the National Oceanographic and Atmospheric Administration (NOAA).

(d) Links will not be made to the home pages of Web sites of private sector news media, magazines, publishers, or radio or television stations. Navy Web sites may, however, list those entities under a heading of media serving the local community, and may link to specific news stories about the DON and/or U.S. joint military operations.

(e) Echelon 2 acquisition commands may link to Web pages of partners in industry provided those Web pages pertain solely and directly to a command program and those links do not constitute nor appear to constitute an endorsement of that partner and/or its products or services. Links may not be made to the partner's main corporate Web site.

(f) Publicly accessible Web sites shall not provide links to content beyond the established access point to restricted sites, so as to not reveal the internal structure.

(10) Web sites using frames will not link to any external content within the window of a frame nor will any Web site prohibit -- through the use of coding -- the visitor to return to a previously visited Web site (i.e., curtailing the use of the "back" button on the browser).

(11) No materials or services may be advertised for sale or sold via a command Web site. This includes command memorabilia, ball caps, etc.

(12) Non-appropriated Fund Activities. Morale, Welfare, and Recreation (MWR) activities are an integral part of nearly every DON command/activities and therefore should have a presence on the command's Web site. This presence shall only contain general information regarding the command MWR program such as patron eligibility, services offered, location of offices, telephone numbers, and hours of

operation. Commercial sponsorship or advertisements shall not be displayed on publicly accessible MWR Web pages.

(13) Information from other military Web sites will not be duplicated but may be referenced or otherwise linked.

4. Exceptions

a. Educational mission. In instances where the mission of the command includes an educational mission, and where unclassified dissertations or professional papers may be published to the Web for the purpose of peer review, the following disclaimer for exchange of professional information and ideas among scientists, physicians, or educators, must be displayed:

"Material contained herein is made available for the purpose of peer review and discussion and does not necessarily reflect the views of the Department of the Navy or the Department of Defense."

b. Recruiting mission. Navy and Marine Corps Recruiting Web sites reside on ".com" domains. These sites may establish procedures for posting and collecting information which differ from all other DON commands/activities, to include advertising their sites on commercial employment opportunity sites. Exceptions to reference (a) must be coordinated through the chain of command as delineated here and in accordance with reference (a).

5. Interactivity. Department of the Navy commands/activities may maintain interactive Web sites to the extent that they allow visitors the ability to query the command via electronic mail (e-mail). Commands/activities are cautioned that establishing and maintaining this interactivity can be extremely labor-intensive. Unmoderated news groups, bulletin boards, or any other unrestricted access posting services are prohibited.

a. Public queries for information should be linked/directed to the site web manager or public affairs office. Queries should be handled consistent with other written requests for information. Responses shall discuss only those issues within the command's cognizance and shall not violate the release of information provisions of references (e) through (g).

b. Commands may link to the U.S. Navy's "Frequently Asked Questions" page on the official U.S. Navy Web site at <http://www.navy.mil>. Questions concerning the U.S. Navy or the

U.S. Marine Corps as a whole shall also be directed to <http://www.navy.mil> or <http://www.usmc.mil> as appropriate.

c. Commands should consider the technical capabilities and needs of their respective audiences when developing the command's Web site. The Information Technology Standards Guide (ITSG) available at <http://www.don-imit.navy.mil/> provides guidance for developing a user-friendly Web site.

d. Command Web sites shall not collect any personal data (name, address, phone number, etc.) about a visitor. Network identification and Internet protocol addresses are not considered personal data. The use of persistent cookies is prohibited on publicly accessible Web sites unless all of the following four conditions are met:

(1) The site provides clear and conspicuous notice of the use of cookies and a description of the safeguards for handling the information collected from the cookies,

(2) There is a compelling need to gather the data on the site,

(3) Appropriate and publicly disclosed privacy safeguards exist for handling any information derived from the cookies; and

(4) The Secretary of Defense personally approves the use of persistent cookies. Requests for approval to use persistent cookies on public Web sites should be submitted to DON CIO at least 90 days prior to operational requirement date, via the appropriate chain of command. The request shall describe the need and the safeguards to be used to protect data, provide an explanation of why other technical approaches are inadequate, and include a copy of the privacy advisory proposed for use.

e. Web Bugs (i.e. tiny and/or invisible graphics on Web pages linked to third-party advertising, marketing, or eavesdropping entities or the like) and other automated means of collecting personally-identifying information without the express permission of the user requires the same approvals as described in paragraph 5d (above).

f. Surveys. The Paperwork Reduction Act of 1995 (PRA) (reference (k)) requires that the collection of information from the public be approved by the Office of Management and Budget (OMB) under certain circumstances.

(1) In accordance with reference (l), surveys requesting identical information from 10 or more members of the public, including DoD/DON contractors, must be approved by OMB. Approval

must be obtained for surveys using check box, radio button, or text form fields. Commands requesting approval from OMB must submit an official letter via the appropriate chain of command to the Office of Management and Budget and must include justification for the proposed survey.

(2) An open-ended offer for visitors to provide comments via a feedback mailto to the web manager does not require OMB approval. However, a clear statement as to the use of this information and to how long it may be retained must be incorporated in the privacy and security notice with a link to that notice.