# Joint Task Force
# National Capital Region Medical
# INSTRUCTION

**NUMBER** 8430.02
DEC 13 2011

J-5

SUBJECT: Website Standards

References: See Enclosure 1

1. PURPOSE. This Instruction, in accordance with the authority in References (a) through (d):

a. Establishes policy, procedures, and best practices for Joint Task Force National Capital Region Medical (JTF CapMed) Webmasters, Web developers, and content managers for developing, reviewing, and publishing JTF CapMed sponsored Web pages in accordance with References (e) through (q).

b. Provides design, content, and publishing standards for public Web sites, as well as information for all Web sites/application in accordance with Reference (k).

2. APPLICABILITY. This Instruction applies to the JTF CapMed and all Joint Medical Treatment Facilities (MTF) and Centers in the National Capital Region (e.g., Fort Belvoir Community Hospital (FBCH), Walter Reed National Military Medical Center (WRNMMC) and Joint Pathology Center).

3. DEFINITIONS. See Glossary

4. POLICY. It is JTF CapMed policy:

a. That content is delivered in a timely manner and accurately on JTF CapMed, FBCH, and WRNMMC public and private Web sites.

b. To communicate a common brand and strategic messages across JTF CapMed, FBCH, and WRNMMC public and private Web sites and Web applications.

c. That all JTF CapMed applicable security policies are applied to all Web sites and applications.

d. To provide a unified entry point to JTF CapMed, FBCH, and WRNMMC unclassified Web resources.

e. To use Web standards set out in this Instruction.

f. To have all public Web site and application reviewed for Operations Security (OPSEC) in February and August of each year. The agency responsible for the Web site will review all of their public Web content for OPSEC compliance and report any findings to JTF CapMed OPSEC office.

g. That the use of the World Wide Web is strongly encouraged; it provides the JTF CapMed with a powerful tool to convey information quickly and efficiently on a broad range of topics relating to its activities, objectives, policies and programs.

h. That the considerable mission benefits gained by using the Web must be carefully balanced through the application of comprehensive risk management procedures against the potential risk to JTF CapMed interests, such as national security, the conduct of federal programs, the safety and security of personnel or assets, or individual privacy created by having electronically aggregated JTF CapMed information more readily accessible to a worldwide audience.

i. That each organization operating a JTF CapMed, Joint MTF, or Center Web site will implement technical security best practices with regard to its establishment, maintenance and administration.

j. That JTF CapMed, Joint MTF, or Center Web sites containing (1) FOR OFFICIAL USE ONLY information, (2) information not specifically cleared and marked as approved for public release in accordance with Reference (f) and DoD Directive 5230.9 (Reference (r)), or (3) information of questionable value to the general public and for which worldwide dissemination poses an unacceptable risk to the JTF CapMed or the Department of Defense, especially in electronically aggregated form, must employ additional security and access controls. Web sites containing information in these categories should not be accessible to the general public.

k. To be consistent with other leadership responsibilities for public and internal communication, the decision whether or not to establish an organizational Web site, and to publish appropriate issuances for a Web site within the limitations established by this document, is hereby delegated to each JTF CapMed Joint MTF and Center.

l. To use Web and Internet-based Capabilities Policies (Reference (s)) as further guidance.

m. That all Domain Name System request or changes must be approved by J-6 Chief Technology Officer.

5. RESPONSIBILITIES. See Enclosure 2

6. PROCEDURES. See Enclosure 3

7. INFORMATION REQUIREMENTS. See Reference (j)

8. RELEASABILITY. UNLIMITED. This Instruction is approved for public release and is available on the Intranet from the JTF CapMed Web site at: www.capmed.mil.

9. EFFECTIVE DATE. This Instruction is effective immediately.

SCOTT WARDELL
Executive Director for Administrative Operations
By direction of the Commander

Enclosures:
1. References
2. Responsibilities
3. Procedures
4. Compliance with Federal, DoD, and JTF CapMed Policy
5. Compliance with Development and Design Standards
6. Guide for Identifying Information Inappropriate for Posting to a Publicly Accessible DoD Web Site
7. Text of Privacy and Security Notice

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES ..... 5

ENCLOSURE 2: RESPONSIBILITIES ..... 7

ENCLOSURE 3: PROCEDURES FOR COMPLIANCE WITH WEB PUBLISHING REQUIREMENTS ..... 10

ENCLOSURE 4: COMPLIANCE WITH FEDERAL, DoD, AND JTF CAPMED POLICY ..... 13

ENCLOSURE 5: COMPLIANCE WITH DEVELOPMENT AND DESIGN STANDARDS ..... 17

ENCLOSURE 6: GUIDE FOR IDENTIFYING INFORMATION INAPPROPRIATE FOR POSTING TO A PUBLICLY ACCESSIBLE DoD WEB SITE ..... 22

ENCLOSURE 7: TEXT OF PRIVACY AND SECURITY NOTICE ..... 24

GLOSSARY ..... 27

ENCLOSURE 1

REFERENCES

(a) Deputy Secretary of Defense Memorandum, "Establishing Authority for Joint Task Force – National Capital Region/Medical (JTF CapMed) and JTF CapMed Transition Team (Unclassified)," September 12, 2007
(b) Deputy Secretary of Defense Action Memo, "Civilian and Military Personnel Management Structures for the Joint Task Force National Capital Region – Medical," January15, 2009
(c) Comprehensive Master Plan for the National Capital Region Medical, April 23, 2010
(d) Supplement to the Comprehensive Master Plan for the National Capital Region Medical, August 31, 2010
(e) DoD Directive 8500.1, "Information Assurance," October 26, 2002
(f) DoD Instruction 8500.2, "Information Assurance (IA)," February 6, 2003
(g) DoD Instruction 5230.29 "Security and Policy Review of DoD Information for Public Release," May 6, 1996
(h) DoD Directive 8320.02, "Data Sharing in a Net-Centric Department of Defense," April 23, 2007
(i) Public Law 106 – 554 – December 21, 2000, 114 STAT. 2753
(j) Defense Information System Agency Web Handbook
(k) DoD Instruction 8910.01, "Information Collecting and Reporting," March 6, 2007
(l) Microsoft Design Guidelines for Developing Class Libraries[1]
(m) Web Server Security Technical Information Guide, V6R1, "DISA Field Security Operations," December 11, 2006
(n) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
(o) DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance," February 12, 2009
(p) DoD Instruction 6025.18, "Privacy of Individually Identifiable Health Information in DoD Health Care Programs," December 2, 2009
(q) Section 508 of the Rehabilitation Act (29 U.S.C. '794 d), as amended by the Workforce Investment Act of 1998 (P.L. 105 - 220), August 7, 1998 (original source in uscode.house.gov)
(r) DoD Directive 5230.9, "Clearance of DoD Information for Public Release," August 22, 2008
(s) Web and Internet-based Capabilities (IbC) Policies[2]
(t) Circular 92 (Copyright Law of the United States and Related Laws Contained in Title 17 of the United States Code)[3].
(u) Section 508 Subpart B, Technical Standards Section 1194.22, "Web-based Intranet and Internet Information Application"
(v) Paperwork Reduction Act (44 U.S.C. 3501 et seq.)[4]
(w) DoD Web Site Administration Policies and Procedures[5]

---

[1] http://msdn.microsoft.com/en-us/library/ms229042.aspx
[2] http://www.defense.gov/Webmasters/policy/dod_Web_policy_12071998_with_amendments_and_corrections.aspx#part1
[3] http://www.copyright.gov/laws/
[4] http://www.archives.gov/federal-register/laws/paperwork-reduction/

(x) DoD Manual 5205.02-M, "Operations Security (OPSEC) Program Manual," November 3, 2008
(y) Carnegie Mellon University Software Engineering Institute, "Security for a Public Web Site," CMU/SEI-SIM-002, August 1997
(z) National Institute of Standards and Technology (NIST), "Internet Security Policy: A Technical Guide."
(aa) Defense Information Systems Agency (DISA), "DISA/NCS World Wide Web (WWW) Handbook Version 2.2," "http://www.disa.mil/handbook/toc.html."
(ab) DoD Chief Information Officer Memorandum, "Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement," May 9, 2008

[5] http://www.defense.gov/Webmasters/policy/dod_Web_policy_12071998_with_amendments_and_corrections.aspx

ENCLOSURE 2

RESPONSIBILITIES

1. JTF CAPMED DIRECTOR, INFORMATION MANAGEMENT/INFORMATION TECHNOLOGY (IM/IT), (J-6). The Director, IM/IT, (J-6), has the responsibility to oversee this Instruction , its policy, and procedures by establishing best practices for JTF CapMed Webmasters, Web developers, and content managers. The Director, J-6, enforces this Instruction through the JTF CAPMED Chief Technical Officer (CTO).

2. JTF CAPMED CTO. JTF CapMed's CTO (J-6) shall:

a. Establish a process for the identification of information appropriate for posting to Web sites and ensure it is consistently applied.

b. Ensure all information placed on publicly accessible Web sites is properly reviewed for security, levels of sensitivity and other concerns before it is released. Detailed requirements for clearance of information for public release are located in References (f) and (r).

c. Ensure approved DoD security and privacy notices and applicable disclaimers are used on all Web sites under their purview.

d. Ensure all information placed on publicly accessible Web sites is appropriate for worldwide dissemination and does not place national security, JTF CapMed or DoD personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

e. Ensure procedures are established for management oversight and regular functional review of the Web site.

f. Ensure operational integrity and security of the computer and network supporting the Web site is maintained.

g. Ensure that reasonable efforts are made to verify the accuracy, consistency, appropriateness, and timeliness of all information placed on the Web site.

h. Register each publicly accessible Web site with the Government Information Locator Service.

i. Ensure that a comprehensive, multi-disciplinary security assessment is conducted of their Web sites within 120 days of the promulgation of this document, and at least bi-annually thereafter.

j. Provide a mechanism for feedback reporting within the Joint MTFs and Centers, to include "Lessons Learned" suitable for JTF CapMed, all Joint MTFs, and Centers.

k. Ensure compliance with this policy for those functions, missions, agencies, and activities in their purview.

2. JTF CAPMED WEB TEAM. JTF CapMed Web Teams shall:

a. Oversee implementation of JTF CapMed, DoD, the Military Health System (MHS) and Federal Web policies.

b. Review all content prior to posting on public Web sites.

c. Establish procedures and standards for command/center Web products.

d. Design, and organize content for www.CapMed.mil that promotes a consistent look and feel on all JTF CapMed, Joint MTF and Center Web products.

e. Maintain agency-level content and coordinates the maintenance of directorate-level content.

f. Research and develop long-term and annual strategies, goals, and objectives for the Agency's use of its Web products; assesses and reports on performance.

g. Manage the agency's Web marketing and outreach efforts.

h. Provide technical assistance in design, operations, and maintenance of JTF CapMed Web pages.

i. Represent JTF CapMed at Web meetings and conferences on Web issues.

j. Provide direction, guidance, and training for JTF CapMed Directorate SharePoint Administrator.

k. Ensure links are operational and outages are resolved.

l. Manage the day-to-day activities on the agency's Web site.

m. Provide the necessary resources (personnel, equipment, dollars) to adequately support Web site operations to include funding, equipping, staffing and training.

3. JTF CAPMED DIRECTORATE LOCAL SHAREPOINT ADMINISTRATOR. The JTF CapMed Directorate SharePoint Administrator shall:

a. Provide overall management of directorate level Web sites.

b. Ensure all Web sites are in compliance with Federal, DoD, MHS, and JTF CapMed Web policy.

c. Periodically review all posted content, including: monitoring for currency, accuracy, and policy alignment; checking for broken links or content errors; and updating contact phone numbers and e-mail addresses.

d. Assist directorate staff with development of Web products or enlists the support of the Joint MTF or Center Web Team.

e. Keep Joint MTF and Center's Web Team up to date on directorate-level Web projects.

f. Coordinate the review and approval of content to be placed on Web products.

g. Engage in archiving and configuration management for directorate Web products.

h. Represent their organization/function at JTF CapMed meetings, conferences, or forums on Web issues.

i. Apply best practices in writing for Web content published via online channels.

ENCLOSURE 3

PROCEDURES FOR COMPLIANCE WITH WEB PUBLISHING REQUIREMENTS

1. WEB PUBLISHING PROCESS – CRITICAL POINTS

a. All Web requests need to be coordinated and submitted through the JTF CapMed Directorate SharePoint Administrator, unless other procedures are established between the Administrator and the Joint MTF and Center's Web Team.

b. The ultimate destination (i.e., CapMed.mil, Patient Tracking System, Intranet) for content is dependent upon the sensitivity and target audience (see Enclosure 5). CapMed.mil will only be used to communicate with the public and JTF CapMed customers – content intended for the JTF CapMed workforce will NOT be published on the public site unless for emergency purposes.

c. Web inventory spreadsheets or automation methods will provide a record of all directorate owned Web pages and sites, including those hosted on public, controlled access, Intranet, and SIPRNet servers. These inventories will be used to assign approval authorities and to conduct bi-annual reviews. It is critical that the spreadsheets be kept up to date to reflect new and deleted pages.

2. DEVELOPING NEW WEB SITES/PAGES/APPLICATIONS

a. Requests for new Web pages, sites, or applications must originate from offices designated as authoritative sources for the information to be published.

b. The JTF CapMed Directorate SharePoint Administrator will coordinate a meeting with the Joint MTF and Center's Web Team and the requesting office (should include subject matter expert). The purpose of the meeting will be to determine:

(1) Site objectives and target audience

(2) Web publishing destination (public, controlled access, intranet, or classified server)

(3) Design, content, and technical requirements

(4) Roles and responsibilities

(5) Schedule

(6) All new pages and sites must be documented in the directorate Web site inventory

3. PRODUCTION/DEVELOPMENT

a. Use of a Web Content Management System is mandatory for the production and maintenance of all pages/sites hosted on JTF CapMed Web resources. Source control software is mandatory for all Web and application development.

b. The Joint MTF and Center's Web Team can take the lead in developing Web pages.

c. If the JTF CapMed Directorate SharePoint Administrator or other directorate staff will be developing or editing Web pages for JTF CapMed's public, controlled access, Web application, or Intranet sites, it is critical to ensure that the programmers tools are properly configured. Please contact the JTF CapMed Web Team if the developer intends on creating and/or revising files from their desktop.

(1) For specific development and design standards, see Enclosure 4.

(2) Development servers may be available for JTF CapMed's public, controlled access, and .net servers to assist with developing and reviewing draft pages and/or sites.

d. For review and approval:

(1) There are three levels of review required for publishing content for the public:

(a) First Level – JTF CapMed Directorate SharePoint Administrator

(b) Third Level – Joint MTF and Center's Web Team/Public Affairs

(c) Fourth Level – OPSEC Manager

(2) There are two levels of review required for publishing content on controlled access and .net servers:

(a) First Level – JTF CapMed Directorate SharePoint Administrator

(b) Third Level – Joint MTF and Center's Web Team and/or Web Site Coordinator

(3) Documentation noting the review and approval by Approval Authority will be submitted. Documentation can take the form of:

(a) Approval Authority's helpdesk request.

(b) Email noting the Approval Authority's review and approval.

(4) The Web Team will coordinate review of materials by the JTF CapMed's Public Affairs Office (PAO) and OPSEC manager. JTF CapMed Directorate SharePoint Administrator will be notified if any modifications are required as a result of the PAO and OPSEC review.

(5) Some content types may require additional review steps not included in this Instruction. When publishing to non-public server, a general rule-of-thumb when determining what content should be submitted for review to the Joint MTF and Center's Web Team:

(a) Content published to controlled-access Web sites intended for working group purposes does not require review/approval by the Joint MTF and Center's Web Team.

(b) Content that offers formal presentation of an official agency position/message destined for publication on any Web site, whether unclassified, controlled access, or classified, must be reviewed/approved by the Joint MTF and Center's Web Team (e.g., marketing materials, factsheets, presentations).

e. For change requests for active pages/sites:

(1) All Web requests must be submitted by the JTF CapMed Directorate SharePoint Administrator unless other procedures are agreed upon between the Joint MTF and Center's Web Team and the JTF CapMed Directorate SharePoint Administrator.

(2) Requests will be submitted using the helpdesk request or e-mail. Minor content changes (e.g., e-mail or phone number updates) do not require approval from Approval Authorities.

f. For semi-annual reviews:

(1) In February and August of each year, each Joint MTF and Center Web Team will review all of their Public Web content for OPSEC compliance.

(2) Reviews will rely upon Web inventory spreadsheets, with each documented page/site requiring review. Once a review is complete, the Joint MTF and Center and Web Team will note completion with an updated "Last Review Date" on their inventory spreadsheets. All finding must be reported to JTF CapMed OPSEC.

(3) See Reference (t) for additional guidance.

(4) Although formal OPSEC reviews will be conducted twice a year, it is expected that all Web content will be reviewed and updated as appropriate.

ENCLOSURE 4

COMPLIANCE WITH FEDERAL, DoD, AND JTF CAPMED POLICY

1. FEDERAL LAWS AND REGULATIONS

a. Section 508 of the Rehabilitation Act (Reference (q)). In 1998, Congress amended the Rehabilitation Act to require Federal agencies to make their electronic and information technology accessible to people with disabilities. Inaccessible technology interferes with an individual's ability to obtain and use information quickly and easily.

(1) Reference (q) was enacted to eliminate barriers in information technology, to make available new opportunities for people with disabilities, and to encourage development of technologies that will help achieve these goals.

(2) The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Under Reference (q), agencies must give disabled employees and members of the public access to information that is comparable to the access available to others.

(3) A person who develops, procures, maintains, services, or uses electronic and information technology (EIT) can at some given point be considered an EIT professional. In particular, conformance to Reference (q) presents many challenges for the Web developer or content manager. Every document, video, image or line of code written must adhere to the standards set for users who fall into the Section 508 categories.

b. Section 508 Standards for the Web. If you need to add additional objects (tables, forms, images, applications, etc.) it is critical to ensure each is accessible. PDF, video and PowerPoint file accessibility is a common issue.

(1) Web-based intranet and internet information and applications (section 1194.22 of Subpart B of Reference (u)).

(a) A text equivalent for every non-text element shall be provided (e.g., via "alt," "longdesc," or in element content).

(b) Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation.

(c) Web pages shall be designed so that all information conveyed with color is also available without color, for example from context or markup.

(d) Documents shall be organized so they are readable without requiring an associated style sheet.

(e) Redundant text links shall be provided for each active region of a server-side image map.

(f) Client-side image maps shall be provided instead of server-side image maps except where the regions cannot be defined with an available geometric shape.

(g) Row and column headers shall be identified for data tables.

(h) Markup shall be used to associate data cells and header cells for data tables that have two or more logical levels of row or column headers.

(i) Frames shall be titled with text that facilitates frame identification and navigation. Pages shall be designed to avoid causing the screen to flicker with a frequency greater than 2 hertz (Hz) and lower than 55 Hz.

(j) A text-only page, with equivalent information or functionality, shall be provided to make a Web site comply with the provisions of this part, when compliance cannot be accomplished in any other way. The content of the text-only page shall be updated whenever the primary page changes.

(k) When pages utilize scripting languages to display content, or to create interface elements, the information provided by the script shall be identified with functional text that can be read by assistive technology.

(l) When a Web page requires that an applet, plug-in, or other application be present on the client system to interpret page content, the page must provide a link to a plug-in or applet that complies with section 1194.21(a) through (l) of Reference (u).

(m) When electronic forms are designed to be completed on-line, the form shall allow people using assistive technology to access the information, field elements, and functionality required for completion and submission of the form, including all directions and cues.

(n) A method shall be provided that permits users to skip repetitive navigation links.

(o) When a timed response is required, the user shall be alerted and given sufficient time to indicate more time is required.

c. Copyright Laws (Reference (t))

(1) Works by the U.S. Government are generally not eligible for copyright protection.

(2) When posting content that is protected by Copyright law, abide by appropriate rules and regulations (Reference (t)).

(3) For questions or concerns regarding copyright law, contact JTF CapMed Chief Counsel/Legal Advisor or the Servicing Legal Office for the Joint MTF or Center as appropriate.

(4) In general, providing a link to a story hosted on the source Web site is permissible. However, republishing a story on a JTF CapMed Web site requires approval from the news source. Contact the Joint MTF and Center's Web Team prior to republishing.

d. Establish required Freedom of Information Act (FOIA) content for publicly accessible sites; including processes to submit FOIA requests, identifying agency FOIA officer, and establishing reading room for common FOIA requests. All JTF CapMed public pages should include a "FOIA" link that is directed to: http://www.capmed.mil/SitePages/FOIA%20Service%20Center.aspx. The link is included within the footer of the JTF CapMed.mil template.

e. The Paperwork Reduction Act provides guidance and requirements for implementation of surveys/questionnaire for which the public may be an audience. See Reference (v).

f. All Federal public Web sites must comply with Reference (i). Information quality requires organizations to publish guidelines for "ensuring and maximizing the quality, objectivity, utility, and integrity of information."

g. All Federal Web sites must comply with existing laws and regulators that address the need to protect the privacy of the American people in accordance with Reference (m). Some of the key requirements include:

(1) Conducting privacy impact assessments

(2) Posting privacy policies

(a) Posting a "Privacy Act Statement" that tells visitors the organization's legal authority for collecting personal data and how the data will be used.

(b) Translating privacy policies into a standardized machine-readable format. Web sites and applications are permitted to use session cookies; however, permanent cookies are not permitted. The only exceptions are those granted by the Secretary of Defense.

(c) All public Web pages must include a link to JTF CapMed's privacy statement: http://www.capmed.mil/SitePages/Privacy%20and%20Security%20Notice.aspx.

h. The standards and specifications for Health Insurance Portability and Accountability Act are as follows and are in accordance with Reference (p):

(1) DoD regulations Web Site Administration Policies and Procedures (Reference (w)).

(a) Unclassified-Sensitive/FOUO information should be placed on Web sites with security and access controls.

(b) Product endorsements or preferential treatment of any private organization shall not appear on any official DoD publicly accessible site -- this includes posting graphics or logos depicting companies/products.

(c) Links to non-DoD Web resources should support organization's mission. A disclaimer is required stating that neither the Department of Defense nor the organization endorses the product or organization at the destination.

(2) Reference (f). Information intended for public release must be reviewed for clearance prior to release.

# ENCLOSURE 5

## COMPLIANCE WITH DEVELOPMENT AND DESIGN STANDARDS

### 1. ENTERPRISE CONTENT MANAGEMENT POLICY

a. The standards for HTML templates and master pages are as follows:

(1) HTML Templates/Master Pages. All JTF CapMed-sponsored public and controlled access Web pages must utilize established HTML templates/master pages. If stated requirements for the Web page or site conflicts with the template requirements, alternate versions can be considered.

(2) Email Addresses. Only generic E-mail addresses (Webmaster@JTFCapMed.mil, program@JTFCapMed.mil, etc.) are permitted on publicly accessible Web sites. No personal E-mail addresses will be published.

(3) Metadata. Keyword and description metadata are required for pages hosted on CapMed.mil. Developers should include the metadata when developing the page. Keywords should be expressed as words or phrases that describe the theme or content of the page or resource. Use the terms someone outside the area would use in a search engine to find information on the Web pages.

(4) Navigation. Site navigation should be along the top and/or down the left side of the page.

(5) Colors. Colors should be consistent throughout the site and represent the organization the site belongs to.

b. Page titles are required for all pages.

c. Links to non-DoD Web resources should support an organization's mission. A disclaimer is required stating that neither the Department of Defense nor the organization endorses the product or organization at the destination. JTF CapMed's link disclaimer is included on the Security, Privacy, and Accessibility page, which is standard footer link on the JTF CapMed Web template. However, when there are several links to private organizations on one page, it is recommended to include the disclaimer in the body of the page.

d. Links to internal systems and Web pages (Intranet, Electronic Data Gathering Equipment, Central Management Information System, etc.) are not permitted on publicly accessible Web sites.

e. Site structure utilizes document-relative pathnames (../index.html) for links and image sources. Absolute pathnames (http://www.CapMed.mil) are not permitted on pages.

f. Web sites and applications are permitted to use session cookies. Permanent cookies are not permitted. Only the Secretary of Defense can grant an exception to this rule.

g. Surveys intended for publication on public Web sites must be coordinated and reviewed by multiple offices within JTF CapMed and/or the Department of Defense.

h. File naming conventions:

(1) Use .html as opposed to .htm

(2) Do not use capital letters in file names and directories

(3) No spaces are permitted within file names

(4) SAMPLE: http://www.JTF CapMed.mil/netwars/index.html

(5) SAMPLE: poc_listing.doc

2. COMPLIANCE WITH CONTENT STANDARDS

a. Personally identifying information, particularly names, pictures, and personal e-mail addresses may not be posted to public Web sites. Exceptions can be made for staff members who, by virtue of their positions, have frequent contact with the public. Contact OPSEC or PAO office for additional guidance.

b. Contact the JTF CapMed Web team with specific questions. Below are guidelines for some of the more frequently asked questions:

c. Dates and times should use the following guidelines:

(1) Military form is appropriate only for dates that are not part of a sentence.

(2) When writing dates, use numerals without th, st, nd, or rd. (e.g., "Nov. 23" NOT "Nov. 23rd")

(3) Spell out the name of the month when using alone, or with a year alone.

(4) When using a specific date, abbreviate the month.

(5) Do not use the year unless it is not the current year.

(6) Use lowercase for a.m. and p.m.

(7) Use a hyphen with no spaces if time spans are inclusive. (e.g., "8-11 a.m." NOT "8 a.m. to 11 a.m.").

(8) Do not use hyphens in a date. For example: The event was held May 12 to 22 (not May 12-22).

d. Phone and fax numbers should be written as follows:

(1) (555) 555-5555, DSN 555

(2) Commercial toll-free numbers with DSN equivalents should be listed (xxx) xxx-xxxx, DSN (zzz) zzz-zzzz

e. Numbers should use the following guidelines:

(1) Spell out a number if it is the first word in a sentence.

(2) Spell numbers below 10. Use numerals for 10 and above.

(3) Use numerals exclusively in dimensions, ratios, proportions, military units, and dates.

f. Acronyms should be spelled out in the first reference, and used only if they appear again in the text.

(1) JTF CapMed does not need to be spelled out on the first reference.

(2) Use DoD for Department of Defense

g. Capitalization should be used as follows:

(1) Only capitalize a title if it is used before a name and is not set off with quotation marks.

(2) Capitalize an item only if it is a major DoD or JTF CapMed program.

(3) Do not capitalize standalone words, such as agency when referring to JTF CapMed or department when referring to Department of Defense.

h. Do not use a hyphen in the names of JTF CapMed field offices. For example: use JTF CAPMED CONUS, not JTF-CAPMED-CONUS.

i. Use e-mail, with the hyphen and no capitalization, unless it begins a sentence or is in a headline.

j. Use "the Web" or WWW in text and www in URLs. To be formal, spell out World Wide Web using initial capital letters. When writing about aspects of the Web, use Web page or Web site.

k. Rules for using "set up" or "setup" and "log on" or "logon."

(1) Use "set up" and "log on" as verbs in instructions, such as "set up the printer" or "log on the network."

(2) "Setup" and "logon" are adjectives or nouns, such as "the setup program" or "your logon password." This rule goes for other similar pairs such as back up and backup.

l. Use "online," not "on-line."

3. WRITING FOR THE WEB. When writing for the Web, ensure that the content meets the following criteria:

a. Target audience is clear.

(1) Who is the intended audience?

(2) What does the audience want to know?

(3) What does the author need to tell them?

b. Purpose of the page is clear and unambiguous.

(1) What is the purpose of this page? State it in the first paragraph.

(2) What does the audience want to know about the subject? What does the author need to tell them?

(3) What should the audience do after they read the page? Is it obvious what the next steps are?

(4) If you anticipate that the audience will want to know something that's beyond the document's scope, include links so that they may find what they're looking for.

c. Content is written and organized efficiently.

(1) Use about 50 percent of the words normally used in print publishing.

(2) To make keywords stand out, use highlighting (bold print).

(3) Highlight only key information-carrying words. Avoid highlighting entire sentences or long phrases.

(4) Bulleted and numbered lists can draw attention to important points.

d. Content is consistent.

(1) Ensure content does not contradict other information on the site.

(2) Avoid duplication and redundancy, except where it is needed to address different audiences.

(3) If information already exists on the Web site about the same subject or about subjects referenced in the document, link to them.

e. Spelling and punctuation are accurate.

f. Content anticipates obvious questions.

(1) What does the audience want to know? What does the author need to tell them? Is all the information there? Did the author anticipate questions? Was the audience led to related materials?

(2) If using acronyms, spell them out on first use.

g. Links add value.

(1) Do links to outside sites add value and/or relate to the site?

(2) Do the words used for links describe the link (no "click here" links)?

h. Graphics add value. No gratuitous graphics that add page weight without content value.

4. FURTHER GUIDANCE. For more guidance see Reference (k).

ENCLOSURE 6

GUIDE FOR IDENTIFYING INFORMATION INAPPROPRIATE FOR POSTING TO A PUBLICLY ACCESSIBLE DoD WEB SITE

1. SECURITY AND ACCESS CONTROLS. Determinations as to the appropriate security and access controls to employ will be based upon the sensitivity of the information and the target audience for which it is intended. Table 1 provides additional guidance to include the vulnerability of various combinations of each. Do not regard these guidelines as the only options available for protecting information content.

Table 1. Security and Access Controls

| If access control is: | and transmission control is: | the vulnerability is: | and the information posted can be: |
|---|---|---|---|
| Open – Includes Webmaster training and certification, isolation of the server, current version of server software and operating system, with all security patches properly installed | Plain text, unencrypted | Extremely High -- Subject to worldwide dissemination and access by everyone on Internet | Non-sensitive, of general interest to the public, cleared and authorized for public release for which worldwide dissemination poses limited risk for DoD or DoD personnel, even if aggregated with other information reasonably expected to be in public domain. |
| Limited by Internet domain (e.g., .mil, .gov) or Internet provider (IP) address | Plain text, unencrypted | Very High -- Can circumvent access controls, affords lowest level of access control, and no encryption | Non-sensitive, not of general interest to the public although approved and authorized for public release, and intended for Department of Defense or other specifically targeted audience. |

| | | | |
|---|---|---|---|
| Limited by user identification (ID) and password (e.g., Defense Management Data Center database or other registration system) | Plain text, unencrypted | High -- Can circumvent access controls, affords higher level of access controls, however, IDs and passwords can be compromised if encryption is not used. | Non-sensitive but limited to a specific, targeted audience. |
| User certificate based (software) requires public key information (PKI) | Encrypted text through use of secure sockets layer | Moderate -- Provides moderate level of access controls | FOR OFFICIAL USE ONLY and information sensitive by aggregation |
| Integrated authentication | Encrypted text through use of secure sockets layer | Low -- Provides good level of access controls | FOR OFFICIAL USE ONLY and information sensitive by aggregation |
| User certificate based (hardware) requires PKI | Encrypted text | Very Low | FOR OFFICIAL USE ONLY and information sensitive by aggregation where extra security is required due to compilation |

2. Refer to Reference (g) for guidance.

3. Until such time as specific technical policy guidelines are formalized for all Internet services, Webmasters and users are encouraged to consult existing authoritative literature on security and access controls. Examples of such literature include, but are not limited to References (y), (z), and (aa).

ENCLOSURE 7

TEXT OF PRIVACY AND SECURITY NOTICE

1. The following privacy and security notice may be tailored in the indicated areas by each organization sponsoring a publicly accessible Web site. The notice shall be approved by the appropriate local legal authority before use.

Link from Index.html pages -- "Please read this privacy and security notice."

( ) - indicates sections to be tailored at the installation level
[ ] - indicates hyperlinks
* - indicates information located at the hyperlink destination indicated

***Quote:***

**PRIVACY AND SECURITY NOTICE**

1. (CapMed.mil Web site) is provided as a public service by the JTF CapMed.

2. Information presented on CapMed.mil is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

3. For site management, [information is collected]* for statistical purposes. This government computer system uses software programs to create summary statistics, which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

4. 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.

5. Except for authorized law enforcement investigations, no other attempts are made to identify individual users or their usage habits. Raw data logs are used for no other purposes and are scheduled for regular destruction in accordance with [National Archives and Records Administration Guidelines].

*Agencies subject to DoD Directive 5240.1 shall add the following to paragraph 5:*

"All data collection activities are in strict accordance with Reference (x)."

6. Unauthorized attempts to upload information or change information on this service are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.

7. If you have any questions or comments about the information presented here, please forward to CapMed.mil [Comment Form]).

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

Cookie Disclaimer. (JTF CapMed) 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. (JTF CapMed) 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. (JTF CapMed) 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 choose 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.

***End Quote:***

* Link from above - "information is collected" to the following text:

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

**Example: Information Collected from (DefenseLINK) for Statistical Purposes**

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

xxx.yyy.com - - [28/Jan/1997:00:00:01 -0500] "GET /DefenseLINK/news/nr012797.html

HTTP/1.0" 200 16704 Mozilla 3.0/www.altavista.digital.com

**xxx.yyy.com (or 123.123.23.12)** -- this is the host name (or IP address) associated with the requester (you as the visitor). In this case, (....com) the requester is coming from a commercial 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.

**[28/Jan/1997:00:00:01 -0500]** -- this is the date and time of the request

**"GET /DefenseLINK/news/nr012797.html HTTP/1.0"** -- this is the location of the requested file on (DefenseLINK)

**200** - this is the status code - 200 is OK - the request was filled

**16704** - 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 (DefenseLINK)

Requests for other types of documents use similar information. No personally-identifying information is collected.

The following notice and consent banner, approved by the DoD Chief Information Officer (Reference (ab)), may be used on all DoD Web sites with security and access controls. This banner may be tailored by an organization but such modifications shall be accomplished in compliance with, and shall be approved by the Component's General Counsel before use.

"This is a Department of Defense Computer System. This computer system, including all related equipment, networks, and network devices (specifically including Internet access) are provided only for authorized U.S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability, and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed or sent over this system may be monitored.

Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject you to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal, or other adverse action. Use of this system constitutes consent to monitoring for these purposes."

# GLOSSARY

## PART 1. ABBREVIATIONS AND ACRONYMS

| | |
|---|---|
| DISA | Defense Information System Agency |
| DoDD | Department of Defense Directive |
| DoDI | Department of Defense Instruction |
| EIT | Electronic and Information Technology |
| FBCH | Fort Belvoir Community Hospital |
| FOIA | Freedom of Information Act |
| FOUO | For Official Use Only |
| JTF CapMed | Joint Task Force National Capital Region Medical |
| OMB | Office of Management and Budget |
| OPSEC | Operation Security |
| PAO | Public Affairs Office |
| WCMS | Web Content Management System |
| WRNMMC | Walter Reed National Military Medical Center |
| WSC | Web Site Coordinators |

## PART II. DEFINITIONS

JTF CapMed Directorate SharePoint Administrator. The person responsible for their department/J-Code Web site content update and interfacing with the Joint MTFs and Centers as well as the JTF CapMed J-6 Web team.

EIT. Includes, but is not limited to, telecommunications products (such as telephones), information kiosks and transaction machines, World Wide Web sites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Health Insurance Portability and Accountability Act (HIPAA) Enacted in 1996. Title I of HIPAA protects health insurance coverage for workers and their families when they change or lose their jobs. Title II of HIPAA, known as the Administrative Standards (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers. The AS provisions also address the security and privacy of health data.

Information Technology. Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

MTFs and Centers. Military Treatment Facilities and Military Treatment Centers.

MTF and Center's Web Team. The Web team that is primarily responsible for the site (FBCH, JTF CapMed, or WRNMMC).

Web Content Management System. A software system which provides Website authoring, collaboration and administration tools designed to allow users with little knowledge of Web programming languages or markup languages to create and manage the site's content with relative ease.