1996

Use of world wide web technologies at the Naval Postgraduate School or NPS internet policy, Draft

Superintendent

Monterey, California: Naval Postgraduate School.

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT

NAVPGSCOLINST XXXX

From: Superintendent
Subj: USE OF WORLD WIDE WEB TECHNOLOGIES AT THE NAVAL POSTGRADUATE SCHOOL or NPS INTERNET POLICY

Ref:

a. NAVPGSCOLINST 5230.4A
b. CINCPACFLT message DTG R 210151Z FEB 98
c. CNO message DTG R 212001Z JUL 95
d. OSD Memo dated July 18, 1997, Establishing DoD Web Information Services
e. OPNAVINST 5239.1B (Draft)
f. NAVPGSCOLINST 5239.1A NPS ADP Security Program (draft)
g. NAVPGSCOLINST 5510.2B NPS Information Security

Encl: (1) Recommendations for web page design and layout

1. Purpose. To establish general Naval Postgraduate School policy governing the operation of World Wide Web Servers on the Internet and NPS Intranet.

2. Cancellation. 1 June 1995 memorandum from acting Associate Provost for Computing and Information Services.

3. Background. Use of Internet/World Wide Web (WWW) technologies provides the Naval Postgraduate School and tenant commands with an efficient means of distributing and collecting information via the Internet and related networks such as extranets and intranets. These technologies are becoming the primary information system in use at NPS. Because the management of the Internet and related networks is distributed, vice centrally controlled, as in a traditional information system, guidance is required for the coordination of resources to provide maximum functionality. This instruction defines responsibilities and standards for the use of WWW technologies at the Naval Postgraduate School.

4. Policy.
   a. Organizational entities at the Naval Postgraduate School may operate HyperText Transfer Protocol (HTTP) or "web" servers in accordance with this instruction, to facilitate the efficient distribution or collection of information. File Transfer Protocol (FTP) servers may also be used. Individual faculty at NPS may operate web services (HTTP and FTP servers) to satisfy instructional/research requirements.

   b. Organizations may operate multiple web servers, but will maintain a single web page that will serve as the top-level page for linking to all related, unclassified organizational information.

   c. The threat of unwanted intrusion into NPS computer systems via the Internet is very high. As a result, Classified and sensitive unclassified information will not be stored on

computers which host anonymous access through Internet web services. Sensitive unclassified material may be accessed via Internet-accessible virtual networks such as extranets or intranets, provided that the information is protected by individual user access control and strong encryption. Reference (f) outlines the NPS network security plan and the process for obtaining Designated Approving Authority (DAA) approval for operating servers that connect to the Internet. Reference (g) provides guidance for the release of unclassified and sensitive unclassified information.

d. Specific restrictions and limitations governing standards of conduct and the appropriate use of NPS computer systems are outlined in reference (a). Failure to comply with reference (a) may result in administrative disciplinary action.

5. Responsibilities. The NPS Internet/Intranet webs are simultaneously considered to be an information system, a digital library, and a public affairs resource. Management of the NPS Internet/Intranet webs therefore requires the coordination of the Computer and Information Services Department (code 05), the Library (code 013), and the Public Affairs Office (code 004).

   a. Code 05 will:
      1. Provide one or more central web servers for all entities at the Naval Postgraduate School to deploy organizational web pages.

      2. Assign and train one or more individuals who will act as the Naval Postgraduate School primary web server administrator or "webmaster"

      3. Determine and publish policy for the operation of web servers at the Naval Postgraduate School.

      4. Maintain a firewall to protect the NPS Intranet from unwanted Internet intrusions or "break-ins".

      5. Take appropriate action to minimize the threat of computer viruses in the web environment. (Ensure that effective anti-virus software is available for all NPS personnel.)

      6. Register the NPS Internet web page with the official Navy webmaster.
   b. The Public Affairs Officer will work with Code in 05 in designing effective content for the NPS Internet web site main pages.

   c. The Director of the Library will determine standards for effective content and structure of the NPS Internet/Intranet webs.

   d. Heads of organizations which maintain an Internet/Intranet presence will:

      1. Assign and train one or more individuals to be the web server administrator for the organization. This is required only for those organizations that operate their own web servers.

      2. Assign and train one or more individuals to be the website administrator for the organization.

      3. Assign and train web page maintainers as necessary.

      4. Ensure that their organization's web site is operated in a professional manner.

e. Users will:
    1. Comply with ref (a).

    2. Take steps to minimize the incidence and spread of computer viruses, such as virus checking all files downloaded from the Internet.

f. Web Server Administrator. Each web server will have one or more web server administrators who are responsible for the administration of that web server. The web server administrator is responsible for:

    1. Operation of the server

    2. Security of the server

    3. Ensuring that designated approving authority (DAA) approval is obtained and maintained, in the case of servers connected to the Internet, in accordance with ref (f).

    4. Establishing procedures for page maintainers to place information on the web server.

    5. Granting and monitoring write access privileges.

    6. Maintaining and evaluating audit control logs

    7. Gathering and analyzing performance data on servers under their control.

    8. Developing, coordinating, publishing, maintaining, and testing support plans for contingency and service restoration.

    9. Implementing security and access controls requested by website administrators or page maintainers.

g. Website Administrator. Each website maintained by an organization will have one or more individuals who are responsible for the administration and appearance of the site. The website administrator billet is often referred to as the "webmaster". The website administrator may also function as the web server administrator. To avoid confusion, be sure to include the organization name when referencing the website administrator, i.e. "NPS Webmaster" or "AA Website Administrator". The website administrator is responsible for:
    1. Maintaining the organization's top level web pages.

    2. Coordinating the structure and appearance of their organization's web.

    3. Ensuring that all links from pages for which they are responsible are appropriate and valid.

    4. Granting and monitoring write access privileges, if applicable.

h. Page Maintainer. Each subordinate page under a website's top level home pages will have a POC identified for information on that page. Page maintainers develop and maintain the information file that resides on the web server. Page maintainers will:

1. Ensure that page content and presentation is consistent with Navy and NPS policy.

2. Ensure that all links from pages under their control are appropriate and valid.

3. If required, ensure proper access and security controls are in place and operational

4. Ensure that outdated or superceded information is removed from the system. If such material is maintained for historical record, ensure that this is clearly indicated.

5. Incorporate a feedback mechanism for user's comments

6. Web page content requirements/restrictions.
   a. Web pages which are accessible via the Internet/NPS Intranet will:
      1. Present a polished and professional appearance.
      2. Support a cohesive, single document structure, branching from the NPS WWW Home Page or Intranet Home Page.
      3. Support intuitive navigation of the entire NPS WWW/Intranet infostructure.
      4. Eliminate duplication.
   b. Organizational home pages will clearly identify their organization and affiliation with NPS.
   c. All links to pages with restricted access will be clearly labeled using the restricted access icon.
   d. Standard disclaimers. The server administrator or page maintainer will include appropriate disclaimers on their pages at the point where they expect readers to enter their information service, usually at the top-level navigational pages. The disclaimers may be in the form of a link. Disclaimers properly apprise users of any restrictions, qualification or implicit permissions associated with the use of such services. Disclaimers also protect the government, the authors and maintainer of services, and the systems administrator(s) of the systems that provide such services by clearly identifying what information represents official policies (as opposed to personal opinions), what routine actions may be ongoing that could be interpreted as infringing on users' privacy, and what consequences may accrue to improper uses. The following statement will be used by all services:

> *This information service operates on a U. S. Government computer system. This system is monitored to ensure proper operation, to verify the functioning of applicable security features, and for other like purposes. Use of this service constitutes consent to such monitoring. Unauthorized attempts to upload or change information; to defeat or circumvent security features; or to utilize this system for other than its intended purposes are prohibited and may result in prosecution under the Computer Fraud and Abuse Act of 1986 or other applicable statutes and regulations.*

In addition, one of the following two disclaimers will be used:

1. By unclassified, non-sensitive organizational information services:

> *This information service is provided by [state name of organization, e.g., the Director of Military Operations at the*

Naval Postgraduate School] for the public viewing and retrieving of information. Unless otherwise indicated, information on this service represents official, unclassified NPS, Department of the Navy, or Department of Defense policies or positions. Information from this service may be distributed or copied, subject only to any indicated copyright restrictions and normally accepted procedures for properly crediting sources.

2. By individual or non-organizational unclassified, non-sensitive information services:

This information service is intended for the public viewing and retrieving of unofficial, unclassified information only. Information on this service should not be construed to represent official NPS, Department of the Navy, or Department of Defense policies or positions. Information from this service may be distributed or copied, subject only to any indicated copyright restrictions and normally accepted procedures for properly crediting sources.

Furthermore, the following disclaimer will be used with any items of unofficial information appearing on an organizational information service:

This information does not represent official NPS, Department of the Navy, or Department of Defense policies or positions.

e. Single source information. Information should remain as closely controlled by the source as possible to ensure its currency and accuracy. Do not copy files from other sources- Reference this information with a link rather than repeat it.

f. Copyright material. Do not use, copy or link to copyright material. This material is usually clearly indicated, but not always. Use caution when using or linking any materials from the Internet.

g. Bandwidth preservation. Reference (a) prohibits "hogging" network resources. Web pages can consume significant bandwidth if not constructed with care. Website administrators and page maintainers must avoid the use of large, high resolution graphics and push technology ("webcasting"). Users will not use push technology clients other than what is provided in the NPS standard workstation configuration.

1. Email. Guidance for the use and operation of email systems at NPS will be contained in a separate instruction.

Enclosure (1)

RECOMMENDATIONS FOR WEB PAGE DESIGN AT THE NAVAL POSTGRADUATE SCHOOL AND TENANT COMMANDS

Prepared by the NPS Web Committee

Top-level web pages should be considered a directory of information contained in subsequent pages and should not contained detailed subject matter. Specifics should reside on subsequent pages

Avoid long lists of hot links on organizational pages… a single link to a separate links page is much more effective.

Top-level organizational pages should have the same "look and feel" so that users will be able to know when they have navigated off of the main pages.

Web pages are dynamic, evolving documents which can frequently change. "Under construction" notices should be used sparingly.

NOTES

Receiving webcasts… refers to users hogging bandwidth. What is a measure of this? How do we know when users are being bad? How do users know? Should we outlaw webcast clients on our net? Assumption:Users will devour whatever bandwidth is made available to them.

What about security??? Instruction must include NIPRNET/SIPRNET… Also, Dean Netzer wishes to publish sensitive unclas material (technical) via the internet, to promote info sharing. It would be protected. Problem is that research coops with faculty at other schools cannot support NIPRNET connections. Need another efficient means to provide information.