



WEB SITE SELF ASSESSMENT CHECKLIST

Updated: 17Dec03

- Ref DOD Web Site Administration Policies and Procedures
A http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html
- Ref SECNAVINST 5720.47A
B <http://www.chinfo.navy.mil/navpalib/internet/secnav5720-47a.pdf>
- Ref NAVADMIN 088/99
C <http://www.bupers.navy.mil/navadmin/nav99/nav99088.txt>
- Ref SECDEF Memo 28DEC2001
D http://www.defenselink.mil/pubs/foi/names_removal.pdf
- Ref SECDEF Memo 13JUL2000
E <http://www.c3i.osd.mil/org/cio/doc/cookies.html>

This document contains a summary of website content requirements and restrictions for publicly accessible Navy websites. A website satisfies the definition of being “publicly accessible” if any of the content on the website is accessible by the public via anonymous access. Restricting access by domain validation or SSL without client-side authentication is not sufficient to be excluded from the definition of “publicly accessible”.

Authorized publicly accessible web presence:

- No entity below the command level or its' equivalent is authorized to establish a publicly accessible web site.**

[Ref B, encl 2: 1.c]

Only commissioned units are authorized to register a domain name for a website. Non-commands are allowed to create a web presence but only as a sub-web off of an authorized web site. Sub-webs will appear as an integral part of their command level parent web site. For instance, sub-webs will be implemented with the same “theme” as the parent web site and any “home” buttons on the sub-web pages must link to the parent’s web site home page only.

Navy publicly accessible web sites MUST:

- Contain the Full command’s organizational name and mailing address.**

[Ref B, encl 2: 2.b.1]

The full command organizational name (with no abbreviations) must be prominently displayed on the web site home page.

- Contain the statement "This is an official U.S. Navy web site".**

[Ref B, encl 2: 2.b.2]

The exact phrase “This is an official U.S. Navy web site” or U.S. Marine Corp must be prominently displayed on the web site home page.

❑ **Contain a tailored Privacy and Security Notice.**

[Ref B, encl 2: 2.b.3; Ref A part V, 4]

The web site Privacy and Security Notice or a hyperlink to the web site Privacy and Security Notice must be prominently displayed on the web site home page.

The Privacy and Security Notice MUST BE verbatim from Refs A or B. The only authorized modifications are to substitute the command's organizational name in the places indicated.

Privacy and Security Notice example per Ref B:

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

1. 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.

2. 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.

3. 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.

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 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."

❑ **Contain the Webmaster contact information.**

[Ref B, 7.d.3]

Information on how to contact the Webmaster must be displayed on the web site home page or at least contained within the source code of the home page. Ideally Webmaster contact information should be listed on the web site home page and should include; an e-mail address, work telephone number and work mailing address.

❑ **Contain a link to parent command or Immediate Superior in Chain (ISIC).**

[Ref B, encl 2: 2.d.2]

❑ **Contain a link to the official U.S. Navy web site: www.navy.mil.**

[Ref B, encl 2: 2.c.1]

❑ **Contain a link to Navy recruiting web site: www.navy.com.**

[Ref B, encl 2: 2.c.3]

❑ **Contain a link to Freedom of Information Act (FOIA) web site: www.foia.navy.mil.**

[Ref B, encl 2: 2.d.4]

❑ **External links to non U.S. Government web sites must be accompanied by a disclaimer statement.**

[Ref A, part II, 8.2 and Ref B, encl 2: 3.d.9]

External links to non-government web sites that directly support the command's mission are authorized but a disclaimer statement must be displayed on the page or pages listing external links or through an intermediate "exit notice" page.

External link disclaimer notice Example:

"The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense, the United States Department of the Navy and [command name] of the linked web sites, or the information, products or services contained therein. For other than authorized activities such as military exchanges and Morale, Welfare and Recreation (MWR) sites, the United States Department of Defense, the Department of the Navy and [command name] does not exercise any editorial control over the information you may find at these locations. Such links are provided consistent with the stated purpose of this DoD web site."

❑ **All solicitations from the web site visitor must be accompanied by a Privacy Advisory.**

[Ref B, encl 2: 5.d; Ref A part II, 12.2]

The term “solicitation” encompasses any and all requests for submissions including surveys, forms, and webmaster feedback.

Privacy Advisory example:

"We will not obtain personally identifying information about you when you visit our site unless you choose to provide such information to us. If you choose to send email to the site webmaster or submit an online feedback form, any contact information that you provide will be solely used to respond to your request and not stored."

- ❑ **Have the written approval of SECDEF for the use of persistent cookies.**

[Reference A, Part II, 12.3.2]

A cookie that is set to expire greater than 24 hours after being set is considered to be “persistent”.

- ❑ **All session cookies and pre-approved persistent cookies must be accompanied by a disclosure statement.**

[Ref A, partII, 12.3.1]

The disclosure statement must state:

- that the site contains a cookie,
- why the cookie is being used,
- the safeguards in place to protect any information collected.

- ❑ **A Notice and Consent Banner.**

[Ref A, part V, 4.2]

A verbatim Notice and Consent Banner (sometimes referred to as a DoD Warning Banner) must be prominently displayed at the access point for web sites where access is controlled by a level 3 Security and Access Control mechanism (ie. User authentication).

Notice and Consent Banner Notice Example:

"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."

Navy publicly accessible web sites must NOT contain:

- ❑ **Overt warning signs, or words of warning or danger in association with the Privacy and Security Notice. The Privacy and Security Notice can only be identified with the phrase “Privacy and Security Notice”.**

[Ref A, part II, 7; Ref B, encl 2: 2.b.3]

Indicators that create a misperception of danger in association with the Privacy and Security Notice will not be used. The Privacy and Security Notice can only be identified with the phrase “Privacy and Security Notice”.

- ❑ **Altered photos (other than standard photographic processes).**

[Ref B, encl 2: 3.b]

Some alterations are acceptable as long as the alterations do not defer from the original intent.

- ❑ **FOUO or above information.**

[Ref A, part V, 2.; Ref B, encl 2: 3.d.1]

- ❑ **Personally identifying content.**

[Ref A, Part V, 2.2; Ref B, encl 2: 3.c.2, 2:3.d.2; Ref D]

Any information that can be used to identify DoD individuals. Exception: Command Executives (ie. CO, XO, CMC) can be identified by photo and name only. The following table lists specific information that is not to be divulged.

Social Security Number	Marital Status	Age
Home address or phone numbers	Birth date	
Race, religion, citizenship	Family members	

- ❑ **Proprietary or copyrighted content.**
[Ref A, Part V, 2.3; Ref B, encl 2:3.d]
- ❑ **Operational Lessons Learned.**
[Ref A, Part II, 3.5.3.1; Ref B, encl 2: 3.d.1]
- ❑ **Information revealing sensitive military operations, exercises, vulnerabilities, maps identifying command and operational facilities.**
[Ref A: part II, 3.5.3.1, 3.5.3.2, Part V, 2.1; Ref B, encl 2: 3.d.1]
- ❑ **Information for specialized, internal audience or of questionable value to the general public that is not access limited by at least domain restriction.**
[Ref A, Part I, 4.3.1, Part II, Part V, 3; Ref B, encl 2: 3.d.3]
Only content that is specifically targeted for the general public should be posted on web sites that have no access restrictions implemented. Content intended for an internal audience will, at a minimum, have access limited by domain restriction.
- ❑ **Information that places national security, personnel, assets, or mission effectiveness at unacceptable risk.**
[Ref A, part II, 3.6.2, part V, 2.; Ref B, encl 2: 3.d.1]
- ❑ **Phone numbers that can be associated with individuals. Only phone numbers for commonly requested resources and services or for office codes are allowed.**
[Ref D, Ref B, encl 2, 3.d.7] should be encl 2, 3.d.7
- ❑ **Product endorsements, preferential treatment of any private organization or product, or references including logo or text indicating that the site is “best viewed” with any specific web browsers.**
[Ref A, part II, 3.5.6, 8.1.2, 8.1.4; Ref B, encl 2: 3.d.4]
- ❑ **Contain links or references to documents within DoD Web sites that have security and access controls.**
[Ref A, Part II, 3.6.3]
However, it is permissible to link to log-on sites, provided details as to the controlled site’s contents are not revealed.
- ❑ **Content duplicated from other military web resources.**
[Ref B, encl 2: 3.d.13]
Navy web sites may reference (via hyperlink) these external resources instead.
For example you may provide a link to: <http://www.chinfo.navy.mil/navpalib/factfile/ffiletop.html> for ship characteristics.