



WEB SITE SELF ASSESSMENT CHECKLIST

Updated: 04Nov2011

- Ref DEPSECDEF Memo 07DEC1998 - Web Site Administration
A <http://www.defense.gov/webmasters/policy/1998-12-7-WebPolicy.pdf> with DoD Web Site Administration Policies and Procedures
http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html
- Ref SECNAVINST 5720.47B, 28 Dec2005 - Department of the Navy Policy for Content of Publicly Accessible World Wide Web Sites
B <http://www.navy.mil/navydata/internet/secnav5720-47b.pdf>
- Ref SECDEF Memo 28DEC2001- Removal of Personally Identifying Information of DoD Personnel from Unclassified Web Sites
C http://www.public.navy.mil/fcc-c10f/nioconorfolk/Documents/names_removal.pdf
- Ref SECDEF Memo 13JUL2000 - Privacy Polices and Data Collection on DOD Public Web Sites
D http://www.public.navy.mil/fcc-c10f/nioconorfolk/Documents/SECDEF13JUL2000_cookies.html
- Ref NTD 08-09, 232200Z JUL 09 (ALCOM 129/09) Policy and Procedures for Web Risk Assessment (WRA) of Publicly Accessible Navy Sites
E <http://www.public.navy.mil/fcc-c10f/nioconorfolk/Documents/NTD-08-09.txt>
- Ref OMB Circular A-130 Management of Federal Information Resources
F <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>
- Ref NAVADMIN 145/07, 051353Z JUN 07, Consolidation of Navy Websites – Reduction of IM/IT Footprint
G <http://www.public.navy.mil/fcc-c10f/nioconorfolk/Documents/NAV07145.txt>
- Ref JTF-GNO CTO 08-012
H <https://www.jtfgno.mil>
- Ref Navy Imagery Decision Tree
I http://www.public.navy.mil/fcc-c10f/nioconorfolk/Documents/navy_imagery_archiving_decision_tree_final.pdf
- Ref OSD Memo 23NOV2010 – Social Security Numbers (SSN) Exposed on Public Facing and Open Government Websites
J https://www.chinfo.navy.mil/socialmedia/OSD_memo_13798-10.pdf
- Ref DoD Memo DTM-08-060 9MAY2008 with change 6SEP2011- Policy on Use of Department of Defense (DoD) Information Systems – Standard Consent Banner and User Agreement
K <http://www.dtic.mil/whs/directives/corres/pdf/DTM-08-060.pdf>
- Ref NAVADMIN 178/11, 091848Z JUN 11, Suicide Prevention Quarterly Update
L <http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMIN/NAV2011/NAV11178.txt>
- Ref Federal Register: July 20, 2006 (Volume 71, Number 139), Rules and Regulations, Page 41095-41099, DOCID:fr20jy06-1
M <http://edocket.access.gpo.gov/2006/E6-11541.htm>

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 [Ref B, 3.d.1] 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 1: 1.e]

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:

❑ **Register/Re-register with NIOC Norfolk.**

[Ref E; Ref B, 7.d.(3)]

Re-registrations are required annually or sooner if any registration information changes (e.g., the webmaster contact information). A Web Site Self Assessment is required prior to registering/re-registering. Note that registration/re-registration addresses SECNAVINST 5720.47B requirement to “designate, in writing, a primary web site manager”. Visit <http://www.public.navy.mil/fcc-c10f/niocnorfolk/Pages/default.aspx> and select Site Checklist and Registration from the Web Risk Assessment pull down menu.

Register the actual site (e.g., <http://www.public.navy.mil/fcc-c10f/niocnorfolk/Pages/default.aspx>) not the site alias (<http://www.nioc-norfolk.navy.mil>).

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

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

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

❑ **Contain a tailored Privacy Policy.**

[Ref B, encl 1: 2.b.3; Ref A part V, 4]

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

The Privacy Policy MUST BE verbatim from Ref A. The only authorized modifications are to substitute the items indicated and to use Privacy Policy versus Privacy and Security Notice. (Note that reference(p) below is left intact here as it relates to the list of references in Ref A of this document.) Links to this tailored privacy policy must be labeled “Please read our Privacy Policy Notice.” as per Ref B.

Privacy Policy example per Ref A:

() - 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. (DefenseLINK) is provided as a public service by the ([Office of the Assistant Secretary of Defense-Public Affairs] and the [Defense Technical Information Center]).
2. Information presented on (DefenseLINK) 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 DoD Directive 5240.1 (reference(p))."

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 them to (us using the DefenseLINK [Comment Form])

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

Cookie Disclaimer. (DefenseLINK) 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. (DefenseLINK) 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. (DefenseLINK) 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.*

- ❑ **Contain the Webmaster contact information.**
[Ref B, encl 1:7.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 Command (ISIC).**
[Ref B, encl 1: 2.d.2]
Please label the link with the text "Parent Command", "Immediate Superior in Command", or "ISIC". This link is required on the home page.
- ❑ **Contain a link to the official U.S. Navy web site: www.navy.mil.**
[Ref B, encl 1: 2.d.1]
This link is required on the home page.
- ❑ **Contain a link to Navy recruiting web site: www.navy.com.**
[Ref B, encl 1: 2.d.3]
This link is required on the home page.
- ❑ **Contain a link to Freedom of Information Act (FOIA) web site: www.foia.navy.mil or foia.navy.mil.**
[Ref B, encl 1: 2.d.4]
This link is required on the home page.
- ❑ **Contain a link to Suicide Prevention Lifeline web site: <http://www.suicidepreventionlifeline.org/Veterans/Default.aspx>.**
[Ref L, 3]
This link is required on the home page. Use the associated icon.
- ❑ **Contain a link to No Fear Act: for example link to http://www.opm.gov/about_opm/nofear/notice.asp or <http://www.public.navy.mil/donhr/Pages/NoFear.aspx>.**
[Ref M, Comments on Notification Obligations]
This link is required on the home page.
- ❑ **External links to non U.S., state, or local government web sites must be accompanied by a disclaimer statement.**
[Ref A, part II, 8.2, and Ref B, encl 1: 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 or [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 or [command name] do 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."
- ❑ **Accompany all solicitations from the web site visitor with a Privacy Advisory.**
[Ref B, encl 1: 6.c.2; 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.**

[Ref A, part II, 12.3.2; Ref B, encl 1:6.a.4]

Cookies that remain after a browser session is terminated are persistent cookies.

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

[Ref A, part II, 12.3.1]

The disclosure statement must state:

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

- ❑ **A Notice and Consent Banner.**

[Ref K, attach 1: A] (supersedes [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 (i.e., User Authentication).

Notice and Consent Banner Example:

"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details."

- ❑ **Ensure all photos have been assigned a Visual Information Record Identification Number (VIRIN) and are properly archived.**

[Ref I]

http://www.public.navy.mil/fcc-c10f/nioonorfolk/Documents/navy_imagery_archiving_decision_tree_final.pdf should be reviewed. Send VIRIN questions to navyvisualnews@navy.mil.

- ❑ **Assist the public in locating government information.**

[Ref F, 8.a.5.(d).(iv)]

Small sites may use site maps or indexes. Larger sites should implement their own search functionality. Note that this requirement can no longer be met by registering with the Government Information Locator Service (GILS) since GILS was discontinued Dec 2005. In addition, the Defense Technology Information Center (DTIC) has discontinued its site crawl support (i.e., www.dtic.mil/dtic/search/submit_site.html is no longer available). Sites may also register at <http://www.defense.gov/RegisteredSites/SubmitLink.aspx>.

- ❑ **Provide accessibility to all U.S. citizens, including persons with disabilities.**

[Ref B, encl 1: 2.c]

Visit <http://www.doncio.navy.mil/section508toolkit/sec0401webbasedaps.htm> for more information.

- ❑ **Register with the DON Application and Database Management System (DADMS).**

[Ref G]

Per NAVADMIN 145/07, all Navy websites must be registered with DADMS. Please see <https://www.dadms.navy.mil> for details. Note that the site is CAC/PKI enabled and also requires a user account. The DADMS Portal/Web site Registration Process Guide is available for those with DADMS accounts. DADMS Helpdesk Support: DADMS@att.com or call (703) 506-5220.

SharePoint sites hosted by another command do not need to register with DADMS. (e.g., NIOC Norfolk’s public site (<http://www.public.navy.mil/fcc-c10f/nioconorfolk/Pages/default.aspx>) does not need to register. In addition, a Navy site hosted by another DoD component does not need to register with DADMS (e.g., NIOC Colorado’s site <http://www.buckley.af.mil/units/nioc>).

- ❑ **Register with the Joint Task Force – Global Network Operations (JTF-GNO).**

[Ref H]

Please visit <https://www.jtfgno.mil> (a CAC/PKI enabled site) for details on Computer Tasking Order 08-012. Failure to register will prevent the site from publishing to the public. Note that this site now presents as US Cyber Forces.

Navy publicly accessible web sites must NOT contain:

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

[Ref A, part II, 7; Ref B, encl 1: 2.b.3]

Indicators that create a misperception of danger in association with the Privacy Policy will not be used. The Privacy Policy can only be identified with the phrase “Privacy Policy”. All references (links) to the Privacy Policy, including the required home page link, shall state: “Please read our Privacy Policy notice.”

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

[Ref B, encl 1: 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 1: 3.d.1]

- ❑ **Personally identifying content.**

[Ref A, part V, 2.2; Ref B, encl 1: 3.c.2, 1:3.d.2; Ref C]

Any information other than name, rank/rate, and duty station that can be used to identify DoD individuals. Exception: Command Executives (i.e., 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	Personal email addresses
Race, religion, citizenship	Family members - except spouses of senior leadership participating in public events	

*To include last four **[Ref J]**.

** For personnel such as the command ombudsman, when a command issued cell phone and/or pager is not available, consider the use of a command number that can either be forwarded to the

ombudsman's personal phone or allow message retrieval.

- ❑ **Proprietary or copyrighted content.**
[Ref A, part V, 2.3; Ref B, encl 1:3.d.6]
- ❑ **Operational Lessons Learned.**
[Ref A, part II, 3.5.3.1; Ref B, encl 1: 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 1: 3.d.1]
- ❑ **Information for specialized, internal audience or of questionable value to the general public.**
[Ref B, 7.d.(1)]
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 cannot be protected by domain restriction alone.
- ❑ **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 1:2.4.c]
- ❑ **Phone numbers that can be associated with individuals. Only phone numbers for commonly requested resources and services or for office codes are allowed.**
[Ref C, Ref B, encl 1, 3.d.7]
Exceptions include Public Affairs Officers, command spokes persons, primary care givers, and chaplains.
- ❑ **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 1: 3.d.3]
- ❑ **Contain links or references to documents within DoD Web sites that have security and access controls.**
[Ref A, part II, 3.6.3; Ref B, encl 1:3.9.g]
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 1: 3.d.13]
Navy web sites may reference (via hyperlink) these external resources instead.
For example you may provide a link to:
http://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=900&ct=4 for ship characteristics for Destroyers or http://www.navy.mil/navydata/fact_display.asp?cid=4200&tid=200&ct=4 for Aircraft Carriers . Note that a ship may publish its own characteristics since the ship has release authority over the data.
- ❑ **Automatic posting of information submitted by unauthorized personnel.**
[Ref B, encl 1: 5a]
Web logs or blogs may not support automatic postings by unauthorized personnel.
- ❑ **Government Information Locator Service (GILS) ID or Number.**
[Ref B, 7.d.3.d]
The Government Information Locator Service (GILS) was discontinued Dec 2005. As a result, NIOC Norfolk no longer uploads registrations to GILS. Unfortunately when SECNAVINST 5720.47B was

published in Dec 2005 it still contained the GILS requirement. The author has been notified and will remove the reference before the next release. Note that the service once provided by the Defense Technology and Information Center (DTIC) via http://www.dtic.mil/dtic/search/dod_search.html is also no longer available.

□ **A Notice and Consent Banner.**

[Ref A, part V, 4.2]

A Notice and Consent Banner (sometimes referred to as a DoD Warning Banner) must NOT be displayed on publicly accessible Navy web sites unless it is associated with an access point for a sub URL where access is controlled by a level 3 Security and Access Control mechanism (i.e., User Authentication).