

TEAMSUB
Web Development Handbook

Aug 23, 2001

Table of Contents

<u>1</u>	<u>INTRODUCTION</u>	2
<u>2</u>	<u>THE NAVSEA NETWORK</u>	2
2.1	<u>ABOUT ZONES</u>	2
2.1.1	<u>Zone 1</u>	2
2.1.2	<u>Zone 2</u>	2
2.1.3	<u>Zone 3</u>	3
<u>3</u>	<u>GENERAL INFORMATION</u>	3
3.1	<u>OBTAINING A DOMAIN NAME</u>	3
3.2	<u>ABOUT DISCLAIMERS</u>	4
3.2.1	<u>Privacy</u>	4
3.2.2	<u>Security</u>	4
<u>4</u>	<u>POSTING TO NAVSEA INTERNET</u>	4
4.1	<u>FUNCTION OF OOD</u>	4
4.2	<u>POSTING</u>	4
4.3	<u>UPDATING THE SITE</u>	4
<u>5</u>	<u>POSTING TO NAVSEA INTRANET</u>	4
5.1	<u>FUNCTION OF SEA 00I</u>	5
5.1.1	<u>SEA 00I Server</u>	5
5.1.2	<u>Non SEA 00I Server</u>	5
5.1.3	<u>Memorandum of Agreement (MOA)</u>	5
5.2	<u>NON-SECURE SITE</u>	5
5.2.1	<u>Posting</u>	6
5.2.2	<u>Updating the Site</u>	6
5.3	<u>SECURE SITE</u>	6
5.3.1	<u>Encryption</u>	6
5.3.2	<u>Obtaining a Certificate</u>	6
5.3.3	<u>Posting</u>	6
5.3.4	<u>Updating the Site</u>	6
5.3.5	<u>Administrative duties</u>	7
<u>6</u>	<u>ABOUT 508</u>	7
<u>7</u>	<u>TASK FORCE WEB</u>	8
	<u>APPENDIX A - GUIDELINES FOR CREATING AND MAINTAINING NAVSEA ORGANIZATION PUBLIC WEBSITES</u>	9
	<u>APPENDIX B - PROCEDURE FOR OBTAINING DOD PKI SERVER CERTIFICATES</u>	23
	<u>APPENDIX C - RISK ASSESSMENT</u>	25
	<u>APPENDIX D - TECHNICAL/SENSITIVE MATERIAL REVIEW FORM</u>	27
	<u>APPENDIX E - DISCLAIMER EXAMPLES</u>	29
	<u>APPENDIX F - EXAMPLE OF A SYSTEM SECURITY AUTHORIZATION AGREEMENT</u>	31
	<u>APPENDIX G - SECTION 508 LINKS</u>	36

1 Introduction

The purpose of this document is to provide contractors and Team Submarine employees with information needed to develop and post a web site or web application to the NAVSEA Internet or Intranet. This document will give a brief explanation of the NAVSEA network structure. It will explain the procedure and guidelines needed to develop and post a web site or web application. This document will assist the contractor or employee to determine where, on the NAVSEA network, to place a web site or web application.

2 The NAVSEA Network

The NAVSEA network consists of several servers. It is these servers that allow employees to communicate via e-mail, share files, store telephone messages, and display web pages. Physical, hardware, and software security measures protect these servers. Because of the versatility of the NAVSEA network, the network is divided into 3 Zones aptly named Zone 1, Zone 2, and Zone 3.

2.1 About Zones

Because of the varied accessibility of the data that resides on the NAVSEA network, zones were created. Each zone has its own level of restrictions from difficult (zone 1) to easy (zone 3). Zone 1 and Zone 2 are behind the NAVSEA firewall. Zone 3 is outside the firewall, which makes it the easiest to access. Figure 1 shows a graphical representation of the zones. Zone 1 has the highest level of restriction, which equates to limited access.

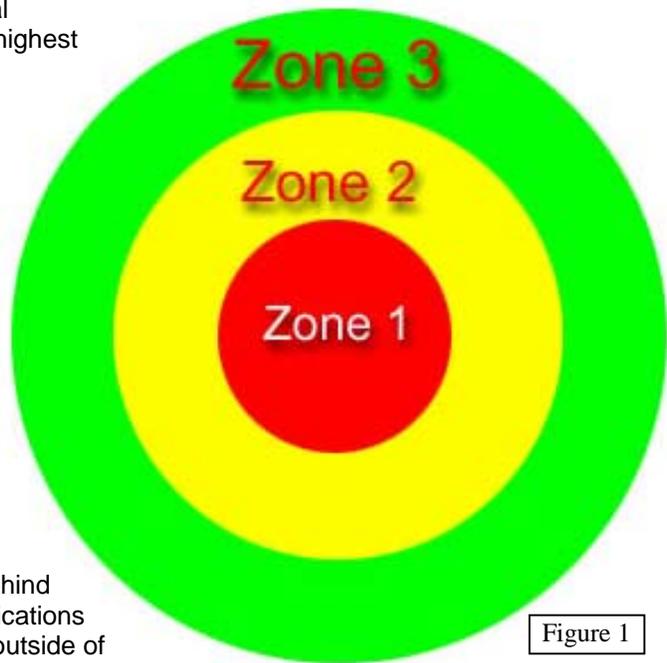


Figure 1

2.1.1 Zone 1

Zone 1 is the backbone of the NAVSEA network. It is only available to NAVSEA Headquarters. Because of its high restriction no web page or web application will be located in this zone. Zone 1 is behind the NAVSEA firewall.

2.1.2 Zone 2

Zone 2 is still behind the NAVSEA firewall but its access restrictions are less than Zone 1. For Intranet access to a web site or web application, that web site or application would be placed in this zone. Although Zone 2 is behind the NAVSEA firewall, web sites and web applications located here can be accessed by individuals outside of the firewall. IP address, Domain name, User ID and Password can restrict access to this zone. There is no direct access to the servers in this zone. No FTP or Telnet will be allowed; access will only be via web browser interactions. Zone 2 is further segmented into 2 parts, 2a and 2b.

2.1.2.1 Zone 2a

Zone 2a can be called a server farm. It consists of several servers containing network and web applications (e.g. Livelink, CDMS).

2.1.2.2 Zone 2b

Zone 2b can be called a web farm. It consists of several servers, containing web sites, web based forms, and web based surveys.

2.1.3 Zone 3

Zone 3, which is outside the NAVSEA firewall, offers the least access restrictions. Web sites and web applications available to anyone surfing the Internet will be placed in this zone. Although it is located outside the NAVSEA firewall, encryption can be used to protect and limit access. Some limited firewall protection is provided by a second firewall box (not NAVSEA's) to discourage hackers.

3 General Information

When developing a web site or web application several factors should be considered before and during development. Some of these factors are:

- Accessibility
- Location of audience
- No Cookies
- No Active-X

Accessibility of the physically challenged to information is now the Law enforced by Section 508 of the Rehabilitation Act (29 U.S.C 794b). Basically it states that individuals with disabilities should have the same or comparable access to and use of information, data and applications that are available to individuals without disabilities. Section 508 will be explained later in this document.

Location of audience is another factor that should be considered when developing a web site or web application. Location of audience will determine the type of restriction needed, zone location, and data content. Data that can be displayed on an Intranet will differ from data that can be displayed on the Internet.

Cookies are small files that can be created by a web site or web application that resides on the computer of a visitor to that web site or web application. They are used to keep track of visitor's preference or personal information. Because of privacy and security concerns, cookies are prohibited.

Because of the security concerns, web site and web applications can't contain Active-X.

Please check Appendix A for NAVSEA Guidelines for Creating and Maintaining NAVSEA Organization Public Websites.

3.1 Obtaining a Domain Name

All web site and web application must have a site or domain name. The naming format of a domain name on a NAVSEA server is as follows:

- http://**sitename**.navsea.navy.mil
- https://**sitename**.navsea.navy.mil
- www.**sitename**.navsea.navy.mil

The location and security of your site will determine the first part of the domain name. "Https" usually indicates a secure web site while 'www' indicates an Internet site. All sites and web applications located on a NAVSEA server will end with "navsea.navy.mil." The "site name" in the domain name must be provided and registered by the owner of the new site or web application.

All site names must be registered with the Information Assurance office. The point of contact is Sylvia Frasier, 202-781-3011.

3.2 About Disclaimers

All NAVSEA hosted web sites or web applications must have links to disclaimers. The nature of the web site or web application will determine the type of disclaimers needed. All web sites and web applications will need a disclaimer stating that the web site or web application is an Official Dept. of the Navy/Government web site or web application.

3.2.1 Privacy

One of the main concerns people have with the web today is privacy. Are they being tracked? If so, what is the information being used for? Privacy for many people is a big concern. A link to a Privacy Disclaimer should be available to assure visitors that their privacy is protected. They should be assured that personal data or personal preferences are not being collected or stored. If personal information and preferences are being collected, a disclaimer should explain why and what will be done with the information collected.

3.2.2 Security

If a web site or web application requires the collection of personal data or personal preference, a link to a security disclaimer should be available. The disclaimer should explain why it is being collected and what will be done with the information collected. The disclaimer should also disclose who has access to the data.

Disclaimers that can be use on a NAVSEA website are located in Appendix E. These disclaimers must be worded exactly as it appears in Appendix E except where noted.

4 Posting to NAVSEA Internet

All information to be posted to the NAVSEA Internet must be submitted to 00D, Public Affairs Office. Codes can only post web pages to the NAVSEA Internet; no web applications are permitted. Web sites to be posted should be stored on a CD or diskette. The CD, printouts (screen shots) of the web site, and a Technical/Sensitive Material Review form (appendix D) should be filled out and given to 00D for review. Although 00D will review the data, it is still the responsibility of the code to ensure that data being submitted for posted meets SECNAV Instruction 5720.47, Department of the Navy Policy for Content of Publicly Accessible World Wide Web Site. This SECNAV instruction can be found at:

<http://www.chinfo.navy.mil/navpalib/internet/5720-47.pdf>

4.1 Function of 00D

The function of 00D is to review the web pages to ensure the information contained within the web pages in the web site is appropriate for viewing by all.

4.2 Posting

Posting will be done by 00D using CD or diskette supplied by the code that developed the web site.

4.3 Updating the Site

Updating the site will be the responsibility of the code that developed the web site via web tools supplied by 00D.

5 Posting to NAVSEA Intranet

All information to be posted on the NAVSEA Intranet will be posted and maintained by SEA 00I, Enterprise Transformation Branch.

5.1 Function of SEA 00I

The function of SEA 00I is to review the information submitted to ensure that the information is in the proper format and meets the general guidelines for a NAVSEA Intranet site, including Section 508. The amount of involvement SEA 00I will have depends on which server is used to store the web pages or applications. Another factor is the way in which access restriction is implemented.

5.1.1 SEA 00I Server

If web pages or applications reside on a SEA 00I server, SEA 00I will be responsible for handling backups, system updates, and posting. Changes to a web site or web application will be the responsibility of the code that developed the web page or web application.

5.1.2 Non SEA 00I Server

If web pages or application reside on a server that does not belong to SEA 00I, the code that supplied the server will be responsible for handling backups and system updates. Depending on the agreement the codes has with SEA 00I, that code may also be responsible for posting new or updated information. Changes to a web site or web application will be the responsibility of the code that developed the web page or web application.

5.1.2.1 Requirements for a Non SEA 00I Server

If a code wishes to supply and use their own server, that code and server must meet the following requirements:

- Server must be rack mountable
- Server must have network software installed (Linux, Microsoft Internet Server, Apache)
- Code must provide manpower to perform general maintenance, software updates, backups, and apply patches.

5.1.3 Memorandum of Agreement (MOA)

A Memorandum of Agreement is a document given to 00I by a code that wishes to post a web site or application on the NAVSEA server. The document clarifies what support the code can expect from 00I and what support the code will provide in maintaining the web site or application. This is established between the code and 00I.

All web sites and applications posted to the NAVSEA Intranet require an MOA that details the following:

- A description of data to include classification.
- Who will provide the data?
- Who will ensure the data content?
- Who will have access to the data?
- If access is limited, how will access be restricted?
- Location of data/server.

In addition to the MOA, a System Security Authorization Agreement (SSAA) will need to be provided. See appendix F for a draft in outline form of a SSAA.

5.2 Non-secure Site

A non-secure Intranet site or application will be accessible to anyone who has access to the NAVSEA Intranet. Access to others can be granted if they can supply a static IP address to SEA 00I.

5.2.1 Posting

To post a web site or application to the NAVSEA Intranet, the site files or application must be given to SEA 00I via a CD or diskette, depending on the size of the site to be posted, and SEA 00I will post it to the NAVSEA Intranet.

5.2.2 Updating the Site

Updates can be sent to SEA 00I via e-mail for SEA 00I to apply updates. Updates can be delivered to SEA 00I via CD, diskette, or Zip disk for SEA 00I to apply updates. Depending on the Memorandum of Agreement, SEA 00I may allow codes access to a terminal so the code can apply changes.

5.3 *Secure Site*

A secure site or application will have limited access. Access to the site or application will be determined by the security plan. The method of limiting access should be detailed in the SSAA. IP address, Domain name, User ID and Password can be used to restrict access. All secure sites and applications require encryption

5.3.1 Encryption

Encryption as defined by the Webster's II New Riverside University Dictionary is "a process for scrambling access codes to prevent illicit entry into a system". In layman's terms, it scrambles data so it is unreadable by anyone without the proper code or key. The encryption is done between the server and the web browser of an authorized user. The server encrypts the data and transmits the data over the Intranet. The web browser of an authorized user decrypts the data for viewing. Anyone who intercepts the data will be unable to view the data. Encryption and decryption are done by using a key. A key is a series of characters, alpha and numeric, that when used with an encryption algorithm encrypts the data. That same key is also used to decrypt the data. Certificates are used to maintain keys used in encrypting and decrypting data. A certificate is a document that must be present on all secure servers. When an authorized user accesses a secure server for the first time, the user is prompted to accept the server's certificate. If accepted, decryption and encryption can take place between the server and the authorized user's computer.

5.3.2 Obtaining a Certificate

All secure servers require a certificate. If it is a new server, the server must be fully built with all software installed before requesting a certificate. All certificate requests are sent to Sharon Heckle (hecklesm@navsea.navy.mil) via e-mail. A one page Risk Assessment should be attached to the e-mail. See Appendix B for details about obtaining a certificate. See appendix C for a template of a Risk Assessment.

5.3.3 Posting

If a code is supplying their own secure server they must make arrangements with SEA 00I to place the server in server farm. The server should contain all necessary files to include the web site or application. If you are placing the Web page or application on an SEA 00I server the site files or application must be give to SEA 00I via a CD or diskette, depending of the size of the site to be posted and SEA 00I will load it on their secure server. A security test plan must be developed and run before access is given to a secure web site or application. The security test ensures that the data or application is secure and no security holes are present that will allow unauthorized access.

5.3.4 Updating the Site

The Memorandum of Agreement and on which server the web site or application is located will determine who will apply updates. If a web site or application resides on a non-SEA 00I server than the code that owns the web site or web application is responsible for updates unless other arrangements are specified in the Memorandum of Agreement. SEA 00I will arrange for codes to

have access to non-SEA 001 servers located in the server farm when updates are required. If a web site or application resides on a SEA 001 server then updates can be sent to SEA 001 via e-mail for SEA 001 to apply updates. Updates can be delivered to SEA 001 via CD, diskette, or Zip disk for SEA 001 to apply updates. Depending on the Memorandum of Agreement, SEA 001 may allow codes access to a terminal so the code can apply changes.

5.3.5 Administrative duties

A secure web site or application requires administrative functions. Methods used to limit access will determine the amount of administrative duties performed. If access is limited by Username and Password, administrative duties would include: setting up and deleting accounts, changing and resetting passwords, and providing assistance for new and old authorized users. If access is limited by IP address, administrative duties would merely include adding and deleting IP addresses. Unless stated otherwise in the Memorandum of Agreement, administrative duties will be performed by the code that developed the web site or application. SEA 001 will provide codes access to the server farm to perform administrative duties.

6 About 508

With the enforcement of Section 508 of the Rehabilitation Act (29 U.S.C 794B), accessibility of a web site and application by the physically challenged is now a major concern. Section 508, as it pertains to web sites and web applications, ensures that individuals with disabilities have the same or comparable access to and use of, information, data and applications that are available to individuals without disabilities. The scope of Section 508 is a large one, too large for this document to cover all aspects. This document will give you the basics needed to develop an accessible web site and application. Links for sites containing further information on Section 508 are listed in Appendix G.

Because the blind can't see where to click or someone with little muscle control can't use a mouse, web site and application developers should ensure that all mouse actions have a keyboard equivalent. If a function is not available using the keyboard, then that function is not accessible. All web sites and applications should be designed so they can be accessed without the use of a mouse.

There are accessibility features built into many operating systems and software. There is the Window's Magnifier accessory software that allows users to enlarge text and graphics on their screen. This aids people that have difficulty seeing small print. Apple's Sticky Key software allows user to do key combinations with one hand or finger. MS Internet Explorer allows users to set the size of the font if the size of the current font is too small to read. When developing a web site or application, ensure that the web site or application does not disable or render these features useless. A web site with a set font size will not allow the user to change the size of the font.

Style sheets are a way to really enhance the format and look of a web page. However, style sheets can disable some of the built in accessibility features. When developing a web site or application that uses styles sheets to enhance the look of a web page, ensure that the web page can be displayed with a style sheet.

Multimedia is another problem for accessibility. Multimedia needs to be available to both the seeing and hearing impaired. If the media is audio, then closed captioning needs to be provided for the hearing impaired. If the media is video, then an audio narrative should be provided for the seeing impaired. If the media is both audio and video, than closed captioning and audio narrative should be provided. It is important that the closed captioning and audio narrative be synced with the audio and video.

Review the Accessibility section of Appendix A for more information concerning Section 508. Useful and informative web links concerning Section 508 can be found in Appendix G.

7 Task Force Web

With the upcoming implementation of the Navy Marine Corp Intranet (NMCI) and the advancement of Internet technologies the future of the Navy as it pertains to distributing, accessing, and manipulating data in support of the Navy/Marine Corp, is the use of portal technologies. The Navy Enterprise Portal will be the one place on the intranet to access the necessary data and applications to support the Navy/Marine Corp mission. In short the term the Navy Enterprise Portal will primarily be used to support the Navy/Marine Corp. In the long term, the Navy Enterprise Portal will be available to Allies, contractors, suppliers, retirees and dependents. Task Force Web (TFW) was established to ensure that web applications developed or applications converted for the web will allow for integration into the Navy Enterprise Portal.

Like Section 508, Task Force Web covers a large scope, too large to be covered in the document. A good site to learn more about Task Force Web is <http://ucso2.hq.navy.mil/n09w>. Developers should refer to this site for addition guidelines for developing a web-based application.

***Appendix A - Guidelines for Creating and Maintaining NAVSEA
Organization Public Websites***

This page intentionally left blank

**Guidelines for Creating and
Maintaining NAVSEA Organization
Websites**

Next page



Guidelines for Creating and Maintaining NAVSEA Organization Websites

Prepared by:

**Deputy Chief Information Officer
Enterprise Architecture
Naval Sea Systems Command**

TABLE OF CONTENTS

INTRODUCTION

RESPONSIBILITY

POLICIES AND PROCEDURES

Appropriateness of Content

Accuracy and Timeliness

Security

Privacy

Domain Names

Notices and Disclaimers

Content Delivery

Usability

Browsers

File Formats

Contact Information

Registration

Accessibility

External Links

Disclaimer for External Links

Images

User Information

Copyrights

Commercial Endorsement

GUIDELINES

User Interface Design Guidelines

Editorial Guidelines

Web Graphic Guidelines

Page Design Guidelines

Site Design Guidelines

Frames

Multimedia

Appendix A. DEFINITIONS

Appendix B. REFERENCES

1. INTRODUCTION

This document contains policies, procedures, and guidelines for the development and administration of public websites deployed by NAVSEA organizations. This document reflects Department of Defense and Department of the Navy instructions and provides guidance that shall be followed by NAVSEA component organizations with respect to establishing, operating and maintaining websites available to the public over the internet.

2. RESPONSIBILITIES

The establishment of a public website on the World Wide Web remains a command prerogative, consistent with other leadership responsibilities for public communication. NAVSEA component organizations choosing to provide public websites shall provide the necessary resources to adequately support website operations to include funding, equipping, staffing and training. The head of each NAVSEA component organization with a public website shall designate a primary website manager, known as the Webmaster, in writing. At a minimum, the Webmaster shall serve as principal point of contact on all technical matters pertaining to administration of the website, oversee the operation of the website, and ensure compliance with appropriate guidelines, directives and instructions. In addition, the Webmaster should monitor the site on a periodic basis, reviewing content and performance of the site as often as possible to ensure no unauthorized changes occur.

3. POLICIES AND PROCEDURES

Appropriateness of Content - The appearance, accuracy, currency and relevance of information presented by NAVSEA component organizations over the Internet reflect upon NAVSEA's professional standards and credibility. The public interprets information associated with a .mil domain as reflecting official Department of Defense policies or positions. Each website sponsored by a NAVSEA component organization shall have a clearly defined purpose that supports the mission of the organizational component. The head of the organizational component or his/her designee shall approve the defined purpose and general content of the websites under their cognizance and establish procedures for regular management oversight and functional review of the website.

Accuracy and Timeliness - NAVSEA component organization websites should contain accurate and timely information. The head of organizational components shall ensure that reasonable efforts are made to verify the accuracy, consistency, appropriateness, and timeliness of all information placed on the website. Effective customer service depends on providing up-to-date information. Out-of-date information should be removed or updated promptly. It is recommended that dates be provided on all web content so users are aware of the date of content posting and the date of expiration if applicable. Dead links inevitably occur on Web sites as pages are modified, moved, or deleted. However, dead links can quickly render a site unusable. Organizations should establish procedures to ensure that the site is frequently monitored for dead links and that such links are corrected as soon as possible. When changing URLs for NAVSEA component organization websites, coordination may be required with other sites, which point to those URLs. When moving a home page to a new URL, NAVSEA component organization Websites should refer users to the new URL or post a message providing the site location.

Security - The head of component organizations shall ensure that all information placed on public websites they sponsor is properly reviewed for security and sensitivity before it is posted. All material posted on public websites should be reviewed and cleared for public release in accordance with the established local procedures in each component organization. All information placed on publicly accessible websites should be appropriate for worldwide dissemination and should be suitable for viewing by anyone any place in the world, both friend and

foe alike. Information on public websites shall not place national security, NAVSEA personnel and assets, mission effectiveness, or the privacy of individuals at an unacceptable level of risk.

Privacy - All NAVSEA component organization public websites shall have a Privacy Statement prominently displayed on any pages that are major entry points to the site. The Privacy Statement shall read:

Of the information we learn about you from your visit to this website, we store only the following: the domain name from which you access the Internet, the date and time you access our site, and the Internet address of the website from which you direct-linked to our site. This information is used to measure the number of visitors to the various sections of our site and to help us make our site more useful. Unless it is specifically stated otherwise, no additional information will be collected about you.

When inquiries or feedback are e-mailed to us, we store the question or comment and the e-mail address information so that we can respond electronically. Unless otherwise required by statute, we do not identify publicly who sends questions or comments to our website. We will not obtain information that will allow us to personally identify you when you visit our site, unless you chose to provide such information to us.

Questions about NAVSEA privacy policies should be sent to the NAVSEA Privacy Act Officer at foia@navsea.navy.mil

Because the electronic mail addresses of site visitors are personally identifying and are generally associated with a specific individual, their compilation into a database or mailing list may present privacy concerns. The use of cookies and the collection of session information may pose privacy concerns to website visitors because the accumulation of this data over time can reveal a visitor's personal preferences and particular interests. If the server to track user information uses cookies across several web pages or web sessions, users should be notified of their use and their purpose.

Domain Names - All NAVSEA component organization public websites must register a domain name. Component organizations should contact (Who?) to coordinate domain name registration. All component organization websites will use the naming convention www.sitename.navsea.navy.mil

Notices and Disclaimers - All NAVSEA component organization websites must contain, at a minimum, the following:

Full organizational name

A statement that the site is an official U.S. Navy website.

A prominently displayed hypertext link to the Privacy Notice identified above and the tailored Security Notice identified below. A statement encouraging visitors to review the security notice is preferred. Overt warning signs or other graphics such as the "skull and crossbones" or "cloak and dagger," or wording indicating danger or warning are specifically forbidden. The tailored Security Notice should be based on the following:

Notice: This is a U.S. Government website. This is a worldwide website for official information about the Naval Sea Systems Command. NAVSEA provides it as a public service. The purpose is to provide information and news about NAVSEA to the general public. All information on this site is public domain and may be distributed or copied unless otherwise specified. Use of appropriate byline/photo/image credits is requested. Unauthorized attempts to upload information or change information on this website are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act. For site security purposes and to ensure that this service remains available to all users, this

government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for authorized law enforcement investigation and to maintain required correspondence files, no other attempts are made to identify individual users or their usage habits. Raw data logs are used to simply determine how many users are accessing the site, which pages are the most popular, and, from time to time, from which top-level domain users are coming. This data is scheduled for regular destruction in accordance with National Archives and Records Administration guidelines.

NAVSEA component organization websites and associated files available for download should carry a Disclaimer of Liability. This disclaimer addresses merchantability and fitness for purpose. In effect, NAVSEA component organization websites need to notify users that there is no implicit warranty for the use of any materials on the website. The following Disclaimer of Liability should appear on NAVSEA component organization websites:

This document was prepared as a service to the NAVSEA community. Neither the United States Government nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process, or service by trade name, trademark manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The opinions of the authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

Content Delivery – NAVSEA component organizations that are sponsoring websites need to decide what forms of material to publish on the site. The World Wide Web offers new opportunities for disseminating electronic materials and resources in a cost effective manner. Instead of publishing only documents, organizations may publish movies, sound, software, electronic data files, and provide interactive experiences for website visitors. Web publishing may complement an existing paper publishing process. However, NAVSEA organizations should consider the new media of the web in determining how and what to publish. A few things to consider are provided below:

Humans interface with computers in a very different way than they do with paper and ink documents. Mere conversion of paper and ink documents to HTML may not be useful to customers. In addition, Hypertext makes many paper and ink conventions obsolete.

Because of the lower resolution on monitors, many users are not interested in reading long documents online but will print them and read them offline. Content to be read online requires authors to write short paragraphs using clear and concise prose.

Effective content delivery provides users with choices. Some content should be viewed, read, or browsed online while other content can best be made available in downloadable files. The choice of file formats used should be based on the following considerations: 1) The intended use of the material by the target audience; 2) The accessibility of the format to the target audience; 3) The type of material; and 4) The level of effort required to convert or prepare the material in the format desired.

The most straightforward way to present material on the web is in HTML or ASCII for text and tables and in GIF or JPEG files for graphics.

Usability – Website developers should focus on the user experience when designing and revising websites. In general, users want clear, easy-to-find information or services, which are delivered as quickly as possible. Whenever possible, NAVSEA Organizations should conduct usability testing to assist in improving the usability of sites.

Browsers – NAVSEA Organization Websites should be designed to work with Netscape and Internet Explorer browsers at least three generations old. The use of features requiring browser plug-ins is optional. Browser plug-ins add capabilities for those users who install them. Often these plug-ins work within the browser expanding its capabilities. These plug-ins accommodate video, audio, vector graphics, and provide other advanced viewing features. Newer versions of browsers recognize programming languages such as JAVA and JAVA Script, which provide interactive options for users. Users of government websites have a wide range of capabilities. Some still use text browsers while others have the latest versions of browsers and all of the plug-ins possible. NAVSEA component organization websites that use browser plug-ins should provide hyperlinks for downloading necessary plug-ins for user convenience and should give the user the option of skipping the portion of the content requiring the plug-in, in the event the user opts not to use it. NAVSEA component organization websites shall not require or encourage users to choose any specific browser software. Only text or hyperlinked text shall be used to direct visitors to software download sites. Graphics or logos depicting companies or products shall not appear on publicly accessible websites.

File Formats - Executable programs available for download from NAVSEA component organization websites should be accompanied with adequate documentation that should include specifications for the platform needed to run the package (i.e., memory, disk space, operating system, etc.), as well as instructions for installation and use. When several files are part of a downloadable collection, content managers may want to make them available in an archive format like .tar, .zip, or .gzip. These formats compress the files to reduce their size, thus speeding up download time. Webmasters should scan all files available for download before posting to ensure that they do not contain viruses.

Contact Information - NAVSEA component organization websites should provide an electronic means for users to contact the sponsoring organization about the technical aspects of the site. This may be accomplished with a hyperlink to the e-mail address of the Webmaster, or a feedback form that captures comments for periodic viewing by the Webmaster. The site should contain a phone number or e-mail address for the public affairs office of the component organization for all other inquiries by the public.

Registration - The Government Information Locator Service (GILS) is an electronic public resource of information throughout the Federal Government. GILS provides user with assistance to the government information through databases, hotlines, clearinghouses and catalogs of publications. All NAVSEA component organization public websites should be registered with GILS. To register, go to website below and follow the directions for filling out the registration form: http://www.itpolicy.gsa.gov/eagency/virtuallibrary/defenseinkhomepageregistration/web_form.html

Accessibility - All NAVSEA component organization public websites must comply with Section 508 of the amended Rehabilitation Act of 1998. This states that all federal agencies must make their electronic and information technology accessible to people with disabilities regardless of the user's computing capability, platform, browser or other disabilities. In order to comply with public law concerning accessibility requirements, all NAVSEA component organization public websites must follow the guidelines below:

A text equivalent for every non-text element shall be provided via "alt" (alternative text attribute), "longdesc" (long description tag), or in element content.

Web pages shall be designed so that all information required for navigation or meaning is not dependent on the ability to identify specific colors.

Changes in the natural language (e.g., English to French) of a document's text and any text equivalents shall be clearly identified.

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

Web pages shall update equivalents for dynamic content whenever the dynamic content changes.

Redundant text links shall be provided for each active region of a server-side image map. Client-side image maps shall be used whenever possible in place of server-side image maps. Data tables shall provide identification of row and column headers. 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. Frames shall be titled with text that facilitates frame identification and navigation. Pages shall be usable when scripts, applets, or other programmatic objects are turned off or are not supported, or shall provide equivalent information on an alternative accessible page. Equivalent alternatives for any multimedia presentation shall be synchronized with the presentation. An appropriate method shall be used to facilitate the easy tracking of page content that provides users of assistive technology the option to skip repetitive navigation links.

For more information concerning Section 508 of the amended Rehabilitation Act of 1998, please visit <http://www.section508.gov/aboutfitai.html>.

External Links - The decision to include a link to an external source should be consistent with sound public policy, in support of our organizational mission, and complement the purpose of the website. External links should be reviewed periodically to ensure their continued suitability. Where appropriate, place external links in context for the user by including statements explaining the purpose of the link. All external links should be clearly identified as such by including the site description and the URL. All NAVSEA component organization public websites should contain the following external links at a minimum:

NAVSEA's official website at <http://www.navsea.navy.mil>

The Navy's official website at <http://www.navy.mil/>

The Navy recruiting site at <http://www.navyjobs.com>

No payment of any kind shall be accepted in exchange for an external link placed on a component organization's public website.

Organizations are encouraged to link to authorized activities in support of the organization's mission. If any linked sites contain commercial advertisements or sponsorships, the disclaimer for external links discussed below shall be given.

When external links to non-government websites are included, the head of the NAVSEA component organization is responsible for ensuring that a disclaimer is made that neither NAVSEA nor the component organization endorses the product or organization at the destination, nor does NAVSEA or the component organization exercise any responsibility over the content at the destination.

Disclaimer for External Links - The disclaimer below shall be displayed when linking to external sites. This disclaimer may appear on the page or pages listing external links, or through an intermediate "exit notice" page generated by the server machine whenever a request is made for any site outside the *sitename.navsea.navy.mil* domain.

"The appearance of hyperlinks does not constitute endorsement by the Naval Sea Systems Command of this website or the information, products or services contained therein. The Naval Sea Systems Command 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 NAVSEA Organization Website."

Images – Official Navy photos that have been cleared for public release may be used on NAVSEA component organization public websites. Official Navy photos may not be altered in any way. Standard photographic practices of cropping, sizing, dodging, or burning are not considered alteration. NAVSEA component organization websites should contain only those images which support the overall mission of the website. All images should have captioning, in accordance with accessibility guidelines discussed elsewhere in this document. Captions should be suitable for

viewing by worldwide audiences. Captions should not contain names or duty addresses of personnel assigned to units that are sensitive, routinely deployable, or stationed in foreign territories.

User Information Collection - Organizations should be careful in collecting information from users. Website users should be notified of any user information collection activities and how the information will be used. There are numerous laws and regulations that govern this activity. Electronic surveys are subject to the provisions of the Paperwork Reduction Act. Any forms that collect information must be cleared by the Office of Management and Budget (OMB) and should have a privacy notice included that describes how the data will be used.

Copyrights - NAVSEA component organization public websites must not contain any material that is copyrighted or under trademark without the specific, written permission of the copyright or trademark holder. A copyright is the 'right' of an author or publisher to the 'copy' (text of an article), which that author or publisher produced. This has come to mean the right of intellectual property, whereby authors obtain, for a specific time, certain exclusive rights to their work. In the United States, and most other countries, a work is copyrighted automatically upon creation. No notice is required nor is registration required with a government agency. NAVSEA component organizations must honor copyright protections. Works prepared by NAVSEA personnel as part of their official duties and posted to organizational websites may not be copyrighted, nor may the website itself be copyrighted.

Commercial Endorsement - In general, the U.S. government does not endorse commercial products or services. However, a reference to a commercial product or service on a government website may be appropriate under certain circumstances. For example, when material in proprietary formats are available for download from NAVSEA Organization Websites, the website should inform the users regarding any commercial software programs that are needed to use the files.

GUIDELINES

The following guidelines are provided to assist NAVSEA component organizations in developing effective websites that reflect credibly upon the NAVSEA enterprise.

User Interface Design Guidelines - Below is a list of common objectives to keep in mind when creating and implementing websites:

The information displayed within a website should answer the Who, What, When, and Where about your project or organization.

Each page should contain a title, creation or revision date, and at least one link to the homepage and the homepage URL or the major menu pages in your site.

Icons and graphics should be easily identified and used consistent throughout the entire site.

Navigation to the major areas in the site should be fairly simple to follow.

Allow for direct access from the homepage to specific information, avoiding unnecessary steps.

Visitors to the site want to gain access to the information quickly.

Optimize the size and number of graphics in accordance with the over-all bandwidth of the website server, assuming most public clients access the Internet at a line speed of 56K.

Websites should maintain a consistent look and feel for each of their pages. For example, the same background should be used throughout the pages of a site to maintain uniformity. Also, titles, subtitles, page footers, links etc. should have a similar style on all pages of the site.

Editorial Guidelines - All information presented in the site should be accurate, clear and to the point. From a design and style perspective, the following styles are recommended:

The main headline should be bold, and have title case capitalization. These include:

Document titles
References to other sites
Titles of other documents mentioned in the site
Proper names, product names, trade names, etc.

Other subheading should be bold and have only the first word capitalized. These include:

References to other sections in the site
Figure titles
Lists of data

The page title should include the name of the NAVSEA component organization, program or project, as well as a brief overview of the information within each page of the site.

Design the link colors to complement the text color.

Check spelling and punctuation of text and make sure all acronyms are in uppercase.

Use standard formatting, fonts and other characters that are supported by HTML based text. Any special formatting technique including "all capitals " produced by style sheets will not convert to ASCII text.

Avoid using different font styles in the website.

When using links to navigate from one page to another within the site, maintain the same graphic design and overall theme to emphasize the link.

The website should have all of the necessary visual effects and text materials to explain the information contained within the framework of the site.

If it is necessary to send the visitor to another website, make sure the background information makes it apparent that they are leaving the primary site.

Maintain the framework of the website for external links by opening new browser windows over the main page, rather than allowing the page to disappear completely. This allows the reader to access other data within a separate window, without losing the visual contact of the main page.

Web Graphic Guidelines

When choosing colors, use the browser safe color palette. It is restrictive in color options, but you must take in consideration that many users have their monitors set to 256 colors, and designs may look differently if other colors are used.

Most personal computers have a resolution that varies between 72 and 96 pixels per inch. Images are limited to the resolutions on each computer screen. When designing graphics, use a 1:1 ratio, where one pixel in the image (ppi) equals one pixel on the screen because this is how an image will display on a web page. Reduce any images that you may use to the 72 ppi before inserting them in the page. When using images and graphics in a website, keep in mind that the more intense the graphic, the slower the downloading time. Compress and minimize graphics used. Web graphics should be .gif or .jpg files.

Include the HEIGHT and WIDTH tags in HTML coding. The tags tell the browser how much space to assign to the graphic on the page. The browser can layout the web page including the graphic space even before the graphics have downloaded.

Use background colors rather than background graphics or complicated textures and patterns. The background colors can change the look of the page without graphics, and overall legibility increases.

Page Design Guidelines

When establishing a page design, consider the overall purpose of the site, the nature of the content, and the expectations of the user.

When images are used, they should be displayed as "thumbnails," which take up less memory and load faster than full-size inline images

Establish a layout grid and a style for handling text and graphics, and then apply it consistently to build rhythm and unity across the pages of the site.

Minimize page scrolling.

Design for discrete screens of information rather than have long text that requires scrolling.

Page headers and footers should be consistent across all pages.

If tables are used for page layout, first define cell widths with absolute values. This will keep the tables from expanding to fill the window. Then, to keep tables from collapsing when the browser window is too small to accommodate their dimensions, include a visible image equal to the width of the cell in each table cell. These two techniques will force table cells to maintain their dimensions regardless of the size of the browser window.

Include standard page elements on the site. Each page should contain a title, an author, an institutional affiliation, a revision date, copyright information, and a link to the "home page" of your site.

Use either plain-color backgrounds or extremely subtle background patterns.

Each web page should contain meta tags (author, subject, title, keyword, description, etc.).

Pertinent web pages should contain appropriate notices (i.e., privacy, disclaimer, security, and/or external link exit notices).

Check the site frequently to ensure that all external and internal links are working.

Incorporate feedback mechanisms. Websites should provide a direct link to the Webmaster responsible for running the site for technical issues, and a link to information regarding how to contact the public affairs office for other questions.

Avoid producing a website that depends on a single browser technology. Minimize the number of browser plug-ins required.

Build "Next Page" and "Previous Page" buttons into your website. This interface tool helps users navigate through the information in your website in the sequence you intended.

Site Design Standards

Incorporate a table of contents, site indexes or site maps in the overall website. Include a frequently asked questions or resource page to direct viewers to sources of information needed. Check all links throughout the website to ensure they are working before you launch the website. Also, run your website using Netscape and Internet Explorer browsers at least three generations old.

Design the website to support multi-platform and cross-platform systems, so that it is viewable by the maximum number of computers and browsers.

Frames

Frames present a more complex way to display your material and preserve the overall design of the site. Using frames, a designer can:

Split the browser screen between information that you want to be present on each screen and other material you want to bring up by a link.

Supply a reader with additional information from another site, while keeping the links from the other site available.

Provide a new page on the viewer's screen, without rewriting the whole screen.

Give the viewer a wider choice in accessing the material.

Frames can also have design limitations. Because the browser window is split from a frame, there is less space on the screen for new content. Careful consideration should be taken when deciding on the overall formatting of the pages with frames so that the viewer is not forced to scroll to see the full content of the page.

Lots of links can be a distraction to the viewer. Place relevant links within the body of the text remembering that these links should open up new browser windows. Place other minor or descriptive links at the bottom of the page, where they are accessible, but not disturbing to the flow of the overall page.

Multimedia

Create content in common standard formats for operating systems and browser software.

Explain to users what browser software and plug-ins are required to use the site or page and provide links to download necessary software and plug-ins.

Use compression to eliminate redundant data and reduce file size.

Appendix A. DEFINITIONS

1. **World Wide Web** - A part of the Internet displaying text and pictures through the use of computer software called a browser. The World Wide Web originated at the European Laboratory for Particle Physics (CERN) in Geneva, Switzerland.
2. **Internet** - A network of networks - a worldwide public network that links many smaller networks. No one owns the Internet. It is funded and managed locally within different countries. Having access to the Internet means being able to send and receive e-mail, partake in interactive conferences, access information resources and network news, and transfer files.
3. **Website** - A website can be thought of as being similar to a "Welcome Aboard" brochure. It describes the organization and its services, and may be a single page or a collection of related, and linked, pages. Information represented on Department of the Navy pages is considered to be official.
4. **Webmaster** - The person who maintains a web page, website, and/or the server upon which the website resides.
5. **Domain** - A part of the Domain Name System. The domain to the farthest right is called the top-level domain. The top-level domain in "www.navy.mil" is ".mil" which stands for military. The domain name for the U.S. Navy is "navy.mil" and the domain name for the U.S. Marine Corps is "usmc.mil". Other top-level domains include ".edu", ".gov", and ".com".
6. **.HTM, .HTML** - The extension for Web documents written in Hypertext Markup Language (HTML) that is the format (code) in which web pages are written. The extension "signals" the browser (reading software) what type of file to decode and display.
7. **Web Page** - An HTML document which is usually served by a Web server. Although a Web page usually contains links to other pages, only the information currently being accessed (i.e., viewed) by a Web browser is a part of the current logical page. The logical page is the building block of a WWW document and is composed of text and possibly graphics and multimedia. The term logical is used because unlike a physical piece of paper, a web page can be as long as needed (from less than one physical page to many physical pages in length). When scrolling down a web page with a browser, the end of the current page is reached when the scroll bar reaches the bottom.
8. **Home Page** - The usual or primary starting (entry) point of a World Wide Web (WWW) site. It is similar to the title page and table of contents of a hard copy document. A home page usually contains links to subsequent (logical) pages in the site. While the home page is the most common access point to a site, it is not the only access point. Any WWW document can be accessed directly from a link or by using its URL (Uniform Resource Locator) address.
9. **Source Code** - The HTML coding which tags and formats the information to make it viewable by the browser. The browser does not normally view the source code.
10. **URL** - Uniform Resource Locator. An Internet "address" of a resource. URLs can refer to web pages, file transfer protocol (FTP) sites or files, Gopher resources, or NNTP (Usenet) Newsgroups. The URLs for pages on the World Wide Web normally begin "http://".
11. **HTTP** - Hypertext Transfer Protocol is the method by which WWW HTML pages are transferred (served) from the Internet to the local computer's Web browser and then displayed.
12. **Link** - A connection from one Web document or file to another, not necessarily within the same website. The link typically appears as a word, or phrase, with blue, underlined letters (Hypertext). As the cursor touches the link, the cursor takes the form of a hand. Clicking the mouse button causes the Web browser to connect to the document pointed to by the link.
13. **Web Browser** - Software that acts as a client, allowing a person to retrieve information from various sources, particularly Web servers.
14. **Web Server** - A software/hardware combination, connected to the Internet, which serves as the "container" for websites and is accessed by Web browser software.

Appendix B. REFERENCES

Americans with Disabilities Act of 1990 (42 U.S.C. 12101 note) and the Rehabilitation Act Amendments of 1992 (29 U.S.C. 794) and General Services Administration Regulation.

Copyright Act of 1976 (Title 17, United States Code, Sections 101-810.) and Copyright Basics, Circular 1, Copyright Office, Library of Congress, Washington, DC, January 1991.

Freedom of Information Act (5 U.S.C. 552).

Amended Rehabilitation Act, 1998, Section 508 (29 U.S.C. § 794d)

Privacy Act (5 U.S.C. 552a).

SECNAVINST 5720.47, "Department of the Navy Policy for Content of Publicly Accessible World Wide Websites"

Deputy Secretary of Defense, Website Administration, Policies and Procedures November 25, 1998

Deputy Secretary of Defense Policy Memorandum, "Government Information Locator Service (GILS), " September 2, 1995

SECNAVINST 5430.97, "Assignment of Public Affairs Responsibilities in the Department of the Navy"

44 USC Chapter 35, "Paperwork Reduction Act", as amended

Appendix B - Procedure for Obtaining DoD PKI Server Certificates

(Provided by Sharon Heckle)

The Information Systems Security Officer (ISSO) for the server will notify the Information Systems Security Manager (ISSM) that a server certificate is needed. Notification will be in the form of an email message with "Server Certificate Request" contained in the subject line. The email message will contain a one-page risk assessment. This risk assessment requests POC information; description of application/server; how it will incorporate PKI; description of the security posture of the system; affirmation that the system has been accredited IAW the DITSCAP and SECNAV/OPNAV INST 5239.1 (see Appendix C). The ISSO will ask that the ISSM endorse and forward the request to the NAVSEA LRA for Server Certificates Sharon Heckel - email address: HeckelSM@navsea.navy.mil.

The system or web administrator for the server requiring a certificate will ensure that the server type and software version can be configured to use DoD issued digital certificates. PKI configuration guides for the more common servers are available at <https://infosec.navy.mil/>.

The system or web administrator will then generate a certificate key pair on the web server. To obtain a server certificate, the administrator (using tools on that server) must generate a NEW certificate request. This process varies among server vendor products and the vendor manual should be consulted. For step-by-step process consult the URL <https://infosec.navy.mil/>. When generating the NEW certificate request, the software will request information - provide the following answers.

Key size:	1024 ONLY
Common Name (CN):	hostname.fully_qualified_domain_name [e.g.: corp.navsea.navy.mil]
Organization:	U.S. Government
Organizational Unit:	DON ou=PKI ou=DoD
Locality:	Leave blank (use a space)
State:	Leave blank (use a space)
Country:	US

NOTE: This process typically requests the operator to create a password-protected file to place the key into.

When the system or web administrator so requests, the NAVSEA LRA will register the server with the Certificate Authority (CA). *Contact the NAVSEA LRA for details.* LRA operators are trained by DCMS or DISA to complete this process. However, the system or web administrator can perform the process of generating a certificate request with the CA, following this procedure below.

You must be using the Domestic version of NETSCAPE 4.05 or higher (128 bit encryption). Follow the instructions carefully to prevent having your Certificate request rejected. The URL for requesting a CLASS 3 DoD PKI certificate is: <http://dodpki.c3pki.chamb.disa.mil/> or http://dodpki.c3pki.den.disa.mil

Select **Request a Server Certificate** (located in the left side frame).

Cut and paste the server certificate request into the text box marked PKCS#10 Request.

Enter Server administrator contact information

The Certificate Authority will automatically e-mail the server administrator directly, after the Registration Authority processes the certificate.

Additional Comments to Issuing Agent should include the following:

NAVSEA LRA: Sharon Heckel
HeckelSM@navsea.navy.mil
Hit **Submit**.

Submit the **your request ID # and full qualifying name of web server (URL)** via email to the NAVSEA LRA.

The NAVSEA LRA will provide the Registration Authority (RA) at DCMS a digitally signed email (preferred) or official message (alternate), the certificate reference number, a brief statement of the purpose of the server, and a statement verifying that the server has been accredited by the cognizant Designated Approval Authority (DAA).

Upon receipt of the information, the RA at DCMS will verify the registration information and approve the issuance of the server certificate. The RA will send the NAVSEA LRA, via email, notification that issuance of the server certificate has been approved.

The Certificate Authority will automatically send an email to the server administrator with the URL to obtain the server certificate.

Using the information provided, the administrator will establish a web connection between the server and the CA, obtain the digital certificate from the CA, and configure the server to utilize the server's private key and digital certificate. This process may differ depending on the type of server and software version being utilized.

Per ALCOM from CNO, the following is the Warning Banner that must be displayed when entering all DoD Systems.

"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 ON 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 ADVERSE ACTION. USE OF THIS SYSTEM CONSTITUTES CONSENT TO MONITORING FOR THESE PURPOSES."

Appendix C - Risk Assessment

(Provided by Sharon Heckel)

This page intentionally left blank

Risk Assessment Template

Next page

Risk Assessment

POC INFORMATION (NAME, ADDRESS, PHONE, FAX, AND E-MAIL ADDRESS)

Example:

Sharon Heckel

Naval Sea Systems Command, 0016

2531 Jefferson Davis Hwy

Arlington, VA 22242

NC2/1W76

Phone: 703 602-xxxx, Fax: 703 602-yyyy

heckelsm@navsea.navy.mil

ONE PARAGRAPH DESCRIPTION OF APPLICATION BEING USED AND ONE PARAGRAPH OF HOW IT WILL INCORPORATE PKI.

Example:

This PKI server certificate will be used for a web server hosting controlled unclassified information for (x) who are the data owners. The purpose of the certificate is to encrypt all the controlled unclassified information from a web server to customers at (y).

ONE PARAGRAPH DESCRIPTION OF THE SECURITY POSTURE OF SYSTEM BEING USED WITH AN AFFIRMATION THAT THE SYSTEM HAS BEEN ACCREDITED IAW THE DITSCAP AND SECNAV/OPNAV INST 5239.1.

Example:

This should state that the system is either fully accredited by the DAA or has an Interim Authority to Operate (IATO). Please include the name of the DAA and the date of the accreditation or IATO. If you are under an IATO, state how long the IATO is good for and when the system will be fully accredited. It should also further state that the SSL enabled by the server would further improve the security posture of the system.

Appendix D - Technical/Sensitive Material Review Form

(Provided by OOD)

This page intentionally left blank

**Technical/Sensitive Material Review
Form**

Next page

Technical/Sensitive Material Review

NAVSEA Public Affairs Office

Due Date:

Activity:

Case Type:

Title:

Please review the enclosed material for technical accuracy and complete the form below. Please do not put in mail. Please return to 00D	Statement A: Approved for Public Release; Distribution is unlimited.
Classification TopSec ___ Sec ___ Conf ___ Unclass ___	Statement B: Distribution authorized to US Government Agencies only; Other request must e referred to COMNAVSEA or the cognizant NAVSEA Code.
Is this intended for electronic dissemination?	Statement C: Distribution authorized to US Government Agencies and their contractors; Other request must be referred to COMNAVSEA or the cognizant NAVSEA Code.
2b. If yes, what form of electronic dissemination will be used?	Statement D: Distribution authorized to DOD and DOD Contractors only; Other request must be referred to COMNAVSEA or the cognizant NAVSEA code
World Wide Web ___ Internet ___ Other ___	Statement E: Distribution authorized to DOD Components; Other request must be referred to COMNAVSEA or the cognizant NAVSEA code.
3. How will release of this hand copy material benefit the Navy? (SECNAVINST 5510.36)	Statement F: Release in not authorized; Further dissemination is only directed by COMNAVSEA or higher authority.

Review: _____ Phone: _____ Code: _____

Recommended Distribution Statement (A - F): ___ Date: _____ Initials: _____

Comments:

Review: _____ Phone: _____ Code: _____

Recommended Distribution Statement (A - F): ___ Date: _____ Initials: _____

Comments:

Review: _____ Phone: _____ Code: _____

Recommended Distribution Statement (A - F): ___ Date: _____ Initials: _____

Comments:

Appendix E - Disclaimer Examples

(Provided by SEA 001)

These disclaimers must be worded exactly as it appears in this Appendix except where noted.

DoD Warning Banner

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 on 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 adverse action. **Use of this system constitutes consent to monitoring for these purposes.**

Intellectual Property Disclaimer

This work is not Public Domain outside of the United States. The Naval Sea Systems Command makes this information available and makes no guarantees that this material is Public Domain. Therefore, reproduction of this material could violate individual copyrights, licensed to the U.S. Government.

Personal Opinion Disclaimer

This document was prepared as a service to the NAVSEA community. Neither the United States Government nor any of their employees, makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process, or service by trade name, trademark manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government. The opinions of the authors expressed herein do not necessarily state or reflect those of the United States Government, and shall not be used for advertising or product endorsement purposes.

The site you are on, NAVSEA Corporate Intranet, is a restricted site. However, all PUBLIC sites shall have the following statements.

Privacy and Security for "Public Websites"

This is an official United States Navy Web Site.

The Department of Defense Resource Locator Record is: _____

This is a worldwide website for official information about the Naval Sea Systems Command. NAVSEA provides it as a public service. The purpose is to provide information and news about NAVSEA to the general public. All information on this site is public domain and may be distributed or copied unless otherwise specified. Use of appropriate byline/photo/image credits is requested. Unauthorized attempts to upload information or change information on this website are strictly prohibited and may be punishable

under the Computer Fraud and Abuse Act of 1986 and the National Information Infrastructure Protection Act. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage. Except for authorized law enforcement investigation and to maintain required correspondence files, no other attempts are made to identify individual users or their usage habits. Raw data logs are used to simply determine how many users are accessing the site, which pages are the most popular, and, from time to time, from which top-level domain users are coming. This data is scheduled for regular destruction in accordance with National Archives and Records Administration guidelines.

Privacy Statement

(Insert Website Name here) is provided as a public service by (insert hosting activity name) and NAVAL SEA SYSTEMS COMMAND.

2. Information presented on (Insert Website Name here) is considered public information and may be distributed or copied unless otherwise specified. 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.
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 1986 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 (insert link to point of contact email).
8. Cookie Disclaimer - (Insert Website Name here) does not use persistent cookies (persistent tokens that pass information back and forth from the client machine to the server). (Insert Website Name here) may use session cookies (tokens that remain active only until you close your browser) in order to make the site easier to use. The Department of Defense DOES NOT keep a database of information obtained from these cookies.

You can choose not to accept these cookies and still use the site, but it may take you longer to fill out the same information repeatedly and clicking on the banners will not take you to the correct link. Refer to the help information in your browser software for instructions on how to disable cookies.

Questions about NAVSEA privacy policies should be sent to the NAVSEA Privacy Act Officer at foia@navsea.navy.mil

Appendix F - Example of a System Security Authorization Agreement
(SSAA)

SSAA TEMPLATE

Outline

SSAA TABLE OF CONTENTS

1.0 MISSION DESCRIPTION AND SYSTEM IDENTIFICATION

- 1.1 SYSTEM NAME AND IDENTIFICATION
- 1.2 SYSTEM DESCRIPTION
- 1.3 FUNCTIONAL DESCRIPTION
 - 1.3.1 System Capabilities
 - 1.3.2 System Criticality
 - 1.3.4 System User Description and Clearance Levels
 - 1.3.5 Life Cycle of the System
- 1.4 SYSTEM CONOPS SUMMARY

2.0 ENVIRONMENT DESCRIPTION

- 2.1 OPERATING ENVIRONMENT
 - 2.1.1 Facility Description
 - 2.1.2 Physical Security
 - 2.1.3 Administrative Issues
 - 2.1.4 Personnel
 - 2.1.5 COMSEC
 - 2.1.6 TEMPEST
 - 2.1.7 Maintenance Procedures
 - 2.1.8 Training Plans
- 2.2 SOFTWARE DEVELOPMENT AND MAINTENANCE ENVIRONMENT
- 2.3 THREAT DESCRIPTION

3.0 SYSTEM ARCHITECTURAL DESCRIPTION

- 3.1 SYSTEM ARCHITECTURE DESCRIPTION
- 3.2 SYSTEM INTERFACES AND EXTERNAL CONNECTIONS
- 3.3 DATA FLOW
- 3.4 ACCREDITATION BOUNDARY

4.0 SYSTEM SECURITY REQUIREMENTS

- 4.1 NATIONAL AND DOD SECURITY REQUIREMENTS
- 4.2 DATA SECURITY REQUIREMENTS
- 4.3 SECURITY CONOPS
- 4.4 NETWORK CONNECTION RULES
- 4.5 CONFIGURATION AND CHANGE MANAGEMENT
- 4.6 REACCREDITATION REQUIREMENTS

5.0 ORGANIZATIONS AND RESOURCES

- 5.1 ORGANIZATION
- 5.2 RESOURCES
- 5.3 TRAINING
- 5.4 OTHER SUPPORTING ORGANIZATIONS

6.0 DITSCAP PLAN

- 6.1 TAILORING FACTORS
 - 6.1.1 Programmatic Considerations
 - 6.1.2 Security Environment
 - 6.1.3 IS Characteristics
 - 6.1.4 Reuse of Previously Applied Solutions
- 6.2 TASKS AND MILESTONES
- 6.3 SCHEDULE SUMMARY
- 6.4 LEVEL OF EFFORT
- 6.5 ROLES AND RESPONSIBILITIES

APPENDIX A ACRONYM LIST

APPENDIX B DEFINITIONS

APPENDIX C REFERENCES

APPENDIX D TRUSTED FACILITY MANUAL

APPENDIX E TOPOLOGY

APPENDIX F REQUIREMENTS TRACEABILITY MATRIX

APPENDIX G CONTINGENCY PLAN

1.0 Mission Description and System Identification

1.1 System Name and identification

1.2 System Description

1.3 Functional Description

1.3.1 System Capabilities

1.3.2 System Criticality

1.3.4 System User Description and Clearance Levels

1.3.5 Life Cycle of the System

1.4 System CONOPS Summary

2.0 Environment Description

2.1 Operating Environment

2.1.1 Facility Description

2.1.2 Physical Security

2.1.3 Administrative Issues

2.1.4 Personnel

2.1.5 COMSEC

2.1.6 TEMPEST

2.1.7 Maintenance Procedures

2.1.8 Training Plans

2.2 Software Development and Maintenance Environment

2.3 Threat Description

3.0 System Architectural Description

3.1 System Architecture Description

3.2 System Interfaces and External Connections

3.3 Data Flow

- 3.4 Accreditation Boundary**
- 4.0 System Security Requirements**
 - 4.1 National and DoD Security Requirements**
 - 4.2 Data Security Requirements**
 - 4.3 Security CONOPS**
 - 4.4 Network Connection Rules**
 - 4.5 Configuration and Change Management**
 - 4.6 Reaccreditation Requirements**
- 5.0 Organizations and Resources**
 - 5.1 Organization**
 - 5.2 Resources**
 - 5.3 Training**
 - 5.4 Other Supporting Organizations**
- 6.0 DITSCAP Plan**
 - 6.1 Tailoring Factors**
 - 6.1.1 Programmatic Considerations
 - 6.1.2 Security Environment
 - 6.1.3 IS Characteristics
 - 6.1.4 Reuse of Previously Applied Solutions
 - 6.2 Tasks and Milestones**
 - 6.3 Schedule Summary**
 - 6.4 Level Of Effort**
 - 6.5 Roles and Responsibilities**

APPENDIX A ACRONYM LIST

APPENDIX B DEFINITIONS

APPENDIX C REFERENCES

APPENDIX D TRUSTED FACILITY MANUAL

APPENDIX E TOPOLOGY

APPENDIX F REQUIREMENTS TRACEABILITY MATRIX

APPENDIX G CONTINGENCY PLAN

Appendix G - Section 508 Links

<http://www.section508.gov> - main government site

<http://www.donogc.navy.mil/lanflt> - Navy's Office of general Council Presentation on 508

<http://www.atlanticfleet.navy.mil/access.htm> - CINCLANTFLT's Website on Section 508

<http://www.army.mil/webmasters/FAQ> - Dept. of the Army Webmasters FAQ Website