



**DEPARTMENT OF THE NAVY**

PERSONNEL SUPPORT ACTIVITY WEST  
937 NORTH HARBOR DRIVE  
SAN DIEGO, CALIFORNIA 92132-0076

PERSUPPACTWESTINST 5230.4B **IN REPLY REFER TO:**

N6

23 Jan 03

PERSUPPACTWEST INSTRUCTION 5230.4B

Subj: INTERNET, INTRANET, AND WORLD WIDE WEB

Encl: (1) Definitions  
(2) Prohibited Uses of Internet Services

1. Purpose. This instruction establishes policy, provides procedures, and assigns responsibilities for using the Internet, Intranet, and World Wide Web (WWW) by all Personnel Support Activity (PSA) West personnel. Additional guidance on the use of the Internet, Intranet, WWW, electronic mail (e-mail), and PSA West network systems is also included. This instruction has been revised in its entirety.

2. Cancellation. PERSUPPACTSANDIEGOINST 5230.4A

3. Applicability. This instruction applies to all PSA West personnel who use U.S. Government-furnished resources to access the Internet, WWW, other government information systems, or the PSA West Internet to access PSA West information systems and services.

4. Definition of Terms. A list of definitions for terms used in this instruction is found in enclosure (1).

5. Policy. The Internet enables users to obtain and exchange information on a global scale. This capability, when used productively, can benefit both PSA West's mission and personnel. Access and use of information services by either Internet or Intranet is granted for conducting official business only. Such use will be monitored to ensure protection of networks and information and to verify compliance with these instructions. All PSA West personnel may also be subjected to unannounced computer inspections under the PSA West Vulnerability Assessment and Analysis Program or other authority. Any violation of this instruction and Internet abuse discovered by any individual will be reported immediately to the Detachment OIC and Systems Administrator (SA). SA will immediately report any violations to the OIC and PSA West Director of Plans and Programs Implementation (DPPI) (N6) and the OIC/N6 will report violations immediately to the PSA West Executive Officer.

a. Content Sensitivity

(1) It is a known fact that criminal, foreign intelligence, and terrorist organizations actively monitor military and technical materials and discussions over the Internet and commercial online service providers. While encouraged to post appropriate materials and documents to the Internet or Intranet, all PSA West personnel must exercise extreme caution to ensure they do not discuss or post any classified, Privacy Act, unclassified sensitive, and contract (procurement) sensitive information. Unclassified information regarding capabilities, vulnerabilities, network topologies, acquisition efforts, policies, and procedures when combined together or with other unclassified (non-sensitive) information can become very sensitive or even classified.

(2) All information posted to the Intranet and/or Internet will be reviewed and approved by the DPPI/N6 prior to release.

b. All PSA West personnel have the inherent responsibility of "stewardship" and must continually promote the safe, effective, efficient, and legal use of all U.S. Government resources. PSA West personnel must:

(1) Exercise the highest standards of professionalism and responsible behavior with the information they obtain from or make available to the Internet or Intranet.

(2) Maximize the use of existing Federal Government Internet servers and the NIPRNET as the means to Internet access.

(3) Act to protect the interests of the taxpayers and the security of the nation. Personnel must also exercise caution and protect information that contractors, foreign governments, or others might use to the disadvantage of PSA West or the U.S. Government. This information may include contractual, operationally sensitive, or Privacy Act information.

(4) Assume that "public" Internet computers can be accessed by anyone worldwide and take action to protect information against unauthorized disclosure.

c. Official Use. Use of PSA West Internet or Intranet services must be work-related and includes all communications determined to be in the interest of the Federal Government and this command. Such use should be appropriate in its frequency and duration, be related to assigned tasks, and include using the Internet or Intranet to:

(1) Obtain or exchange information to support DON or PSA West missions.

(2) Obtain or exchange information that enhances the professional skills of PSA West employees and benefits the command and job performance within the command.

(3) Improve professional or personal skills as part of a formal academic education or military or civilian professional development program (when approved by the OIC).

d. Government computers may be used to access the Internet for incidental personal purposes such as brief communications, brief Internet searches, and other uses allowed as long as such use:

(1) Does not adversely affect the performance of official duties by the DOD employee or the DOD employee's organization.

(2) Serves a legitimate public interest such as enhancing professional skills, educating DOD employees in using the system, improving morale of employees stationed away from home for extended periods, or job-searching in response to Federal Government downsizing.

(3) Is of minimal frequency and duration and occurs during an employee's personal time.

(4) Does not overburden Federal Government computing resources or communications systems nor does not result in added costs to the Government.

(5) Is not used for purposes that adversely reflect on this command and the Federal Government. A listing of prohibited uses of information services is in enclosure (2).

6. Information and the Internet. Users may obtain or exchange information using Internet host capabilities such as electronic mail (e-mail), WWW, Remote Access Service (RAS), File Transfer Protocol (FTP), or Telecommunications Network (TELNET) services. This information may be categorized as publicly releasable, limited release, or Privacy Act information.

a. Publicly releasable information is any information made available to the general public without security or access controls. It must be unclassified, operationally nonsensitive, related to PSA West's mission, and consistent with the intent of the Freedom of Information Act. Publicly releasable information will be maintained and made available primarily through PSA West's "external" WWW servers or, when appropriate, through other publicly accessible Internet hosts.

b. Limited release information includes PSA West-business or other "For Official Use Only" (FOUO) information, products with specific licensing or use restrictions, and source selection-sensitive or proprietary information. It may not include classified information. Limited release information will not be made available to the general public. Limited release information made available to activities outside PSA West must have appropriate user registration procedures, user ID, and password controls.

c. Privacy Act information identifies or describes a person and requires that person's permission for release outside official DOD channels. Privacy Act information generally will not be made available on the Internet or Intranet. When operational requirements mandate the use of Privacy Act information using the Internet or Intranet, it must be properly protected.

d. Material proposed to be made available electronically to the publicly accessible Internet or the more restricted Internet must be submitted either in written hard copy or via e-mail to DPPI/N6 prior to release.

7. PSA West Information Release and Review Authorities. All information to be posted to a PSA West Internet or Intranet host, whether for public or limited release, must undergo organizational and command-level reviews. All information must be reviewed and approved by the DPPI/N6 prior to posting to a PSA West Internet or Intranet server.

8. PSA West Internet Services. All PSA West employees will be given full Internet access and must comply with the following procedures:

a. PSA West will not provide RAS or other specialized network access, unless deemed mission essential by the DPPI/N6.

b. E-mail and FTP Services

(1) All personnel must ensure that the content of their e-mail messages is professional and does not misrepresent or misstate command or DOD positions or policies.

(2) Obtaining executable software from FTP sites outside DOD and other governmental agencies is discouraged.

c. Only designated personnel within N6 and the PSD Systems Administrator are authorized to download software. PSA West personnel will not download commercial software or "shareware," unless it is used for evaluation only and approved by DPPI/N6. All users must ensure that downloaded software is properly screened and cleared of viruses before storing software or data on PSA West network resources. Users must also be aware of network disk storage limitations and consider such limitations before storing files or data on network resources.

d. Shareware-like commercial software may be purchased and used when properly obtained through established command acquisition processes.

e. PSA West users are not authorized to utilize Internet chat, instant messaging, web-based e-mail, and phone functions of the Internet.

f. PSA West personnel may browse the Internet but must avoid all unproductive sites.

9. PSA West World Wide Web (PSA West WWW). The PSA West WWW will be the primary means for PSA West uses to share information with the general public. All information presented on the PSA West WWW is the direct responsibility of the senior management within department and Detachment. These persons must ensure that all information is kept current and that all PSA West WWW resources, which are no longer required, are properly released.

10. Procedures

a. All requests for Internet and Intranet access and service requirements must be submitted to PSA West DPPI for approval.

b. All PSA West web pages will be developed using the following procedures:

(1) All information to be presented on a PSA West web page must be approved by the DPPI. This approval must be documented either by letter or by e-mail. When practical, include an exact representation of the information to be presented especially when using resources directly managed by the PSA West Webmaster.

(2) Once the organizational information is approved and assembled, forward it to the PSA West Webmaster for PSA West web services and postings.

11. Responsibilities

a. All PSA West personnel are responsible for promoting the effective and efficient use of the PSA West Internet, Intranet, and WWW services. All PSA West personnel will:

(1) Ensure that all information provided to PSA West Internet and Intranet hosts reflects the highest standards of quality and utility.

(2) Report all suspected intrusions or compromises of PSA West Internet or Intranet services, controls, or any suspected alterations of the information PSA West makes available on its Internet hosts. Direct these reports to the DCCS, PSA West Network Manager, or to the PSA West Webmaster.

(3) Abide by all patent, copyright, trade secret, and licensing agreements in their use of software, services, or information obtained from Internet.

  
CAROLINE E. KONCZEY

Distribution:

PERSUPPACTWESTINST 5216.1K, Lists I and II

**DEFINITIONS**

Basic Internet Services. In this publication, Internet services refer to the general Internet capabilities provided to the typical PSA West user. These services are provided within established PSA West Network resources and typically include e-mail capabilities to Internet and Intranet addressees. Internet services are predominantly user-level services.

External Server. An Internet host computer system that is accessible by the general public without user access controls such as user IDs and passwords.

File Transfer Protocol (FTP). A software protocol that facilitates transfer of files between Internet users and systems.

Internet. A collection of a worldwide "network of networks" that uses the Transmission Control Protocol/Interface Protocol (TCP/IP) for communications. The Internet includes resources that span academic, business, government, and personal interests.

Internet Chat. Systems that allow users to exchange text interactively over the Internet.

Internet Host. Any computer or computer network that serves as a repository for services available to other computers on the Internet. Internet hosts typically offer services such as e-mail, file transfers protocol, web, or text search services.

Internet Phone. Systems designed to present real or near-real time voice over the Internet.

Intranet Server. Refers to a server that uses security or access controls to strictly limit access to users from within an agency, organization, or company by employing security features such as firewalls to control access to other Internet and Intranet servers and authorized Intranet users.

PSA West Internet. Refers to interconnection of PSA West owned and operated networks or computers with access to the Internet. These systems are not the same as the Internet, but rely on the Internet to connect PSA West-owned systems with other non-PSA West networks.

PSA West Intranet. Refers to PSA West-owned and PSA West-operated networks or computers with restricted access from the WWW and Internet through the use of security or access controls to essentially create a private or limited access network using the Internet protocols and services. This network's users are strictly limited to be within PSA West and/or its components.

PSA West World Wide Web (WWW). The complete collection of hardware and software owned and operated by PSA West that provide PSA West's presence on the WWW and provide PSA West users with hypertext protocol features and services.

Sensitive Information. Information for which loss, unauthorized modification, or unauthorized disclosure would be detrimental to command operations. Sensitive information may be personal, proprietary, financial, national security-related, or critical to command plans and operations. In this instruction, the term limited release information provides an equivalent meaning.

Shareware. Copyrighted software that has been developed and placed in the public domain or in general circulation to increase public use. The developer of such software usually requests a nominal fee using the honor system for the software and its future updates.

Special Services. Refers to Internet services that extend beyond user-level requirements. Special services may include specialized connections to the Internet, hardware and software to operate a server, or communications support such as dial-in lines to access an Internet host or gateway.

Telnet. An Internet capability that allows a user to connect to another Internet computer and use that system remotely.

Web Page. A page of information typically presented using the hypertext markup language (HTML) and accessible using the World Wide Web. Web pages may present a variety of information sources from text to a combination of sound, graphics, and video.

Web Server. The collection of hardware, software, and data using World Wide Web technology and hypertext markup language as the means to navigate between web servers and the documents and resources available on these servers.

World Wide Web. An Internet service that permits users to weave information and resources together by using hypertext links.

**PROHIBITED USE OF INTERNET SERVICES**

1. The use of Internet services in the following types of activities is specifically prohibited:
  - a. Illegal, fraudulent, or malicious activities.
  - b. Partisan political activity, political or religious lobbying or advocacy, or activities on behalf of organizations having no affiliation with PSA West or DOD.
  - c. Activities whose purposes are for personal or commercial financial gain. These activities may include chain letters, solicitation of business or services, and sales of personal property.
  - d. Unauthorized fund raising or similar activities, whether for commercial, personal, or charitable purposes. Official morale, welfare, recreation, officer, and enlisted aid activities are authorized.
  - e. Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.
  - f. Storing, processing, or distributing classified, proprietary, or other sensitive or FOUO information on a computer or network not explicitly approved for such processing, storage, or distribution.
  - g. Annoying or harassing another person, e.g., by sending or displaying uninvited e-mail of a personal nature or by using lewd or offensive language in an e-mail message.
  - h. Using another person's account or identity without his/her explicit permission, e.g., by forging e-mail.
  - i. Viewing, damaging, or deleting files or communications belonging to others without appropriate authorization or permission.
  - j. Attempting to circumvent or defeat security or auditing systems without prior authorization and other than as part of legitimate system testing or security research.
  - k. Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's patent, copyrights, trade secret, or license agreement.
  - l. Permitting any unauthorized person to access a PSA West or DOD-owned system.
  - m. Modifying or altering the operating system or system configuration without first obtaining permission from the owner or administrator of that system.

n. Accessing instant messaging, Internet chat, and web based e-mail from a government owned or leased system or network.

2. These activities may result in administrative or other disciplinary action such as actions mandated by the Uniform Code of Military Justice, nonjudicial punishments, performance appraisals, and personnel disciplinary actions.