DEFENSE INFORMATION SYSTEMS AGENCY
701 S. COURTHOUSE ROAD
ARLINGTON, VIRGINIA 22204-2199

COMP-00010

DISA INSTRUCTION 630-225-7* 6 September 1996

INFORMATION SERVICES

Internet, Intranet, and World Wide Web

1. **Purpose.** This Instruction establishes policy, provides procedures, and assigns responsibilities for using the Internet, Intranet, and World Wide Web (WWW) by Defense Information Systems Agency (DISA) organizations, personnel, and contractors. It provides additional guidance on the use of the Internet, Intranet, WWW, electronic mail (e-mail), and DISA Network (DISANet) systems.

2. **Applicability.** This Instruction applies to all DISA and Office of the Manager, National Communications System (OMNCS), personnel and DISA contractors who use U.S. Government-furnished resources to access the Internet, WWW, other government information systems or the DISA Intranet to access DISA information systems and services.

3. **References.**

3.1 DPL 96-6, Information Services, 5 September 1996.

3.2 DOD 5500.7-R, Joint Ethics Regulation, 3 April 1996.

3.3 DISAI 630-230-19, Information Systems Security Program, 9 July 1996.

3.4 DISAI 240-225-1, Clearance of DOD Information for Public Release, 18 February 1983.

3.5 DOD Directive 5230.9, Clearance of DOD Information for Public Release, 9 April 1996.

3.6 Deputy Secretary of Defense Memorandum, Clearance Procedures for Making Electronic Information Available to the Public, 17 February 1995.

3.7 DISA Interoffice Memorandum, CIO, DISA Information System (DISA-IS) Requirements Process, 22 February 1994.

3.8 DISA Acquisition How-To-Guide, August 1993. (OPR: D41)

3.9 DISA CIO Memorandum,. Standardized DISA E-Mail Addresses, 10 April 1995.

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 06091996	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle DISA Instruction 630-225-7, Information Services: Internet, Intranet, and World Wide Web	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) IATAC Information Assurance Technology Analysis Center 3190 Fairview Park Drive Falls Church VA 22042	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 17	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	9/6/96	Instruction

4. TITLE AND SUBTITLE
DISA Instruction 630-225-7, Information Services: Internet, Intranet, and World Wide Web

5. FUNDING NUMBERS

6. AUTHOR(S)
DISA

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

Purpose. This Instruction establishes policy, provides procedures, and assigns responsibilities for using the Internet,
Intranet, and World Wide Web (WWW) by Defense Information Systems Agency (DISA) organizations, personnel, and contractors. It provides additional guidance on the use of the Internet, Intranet, WWW, electronic mail (e-mail), and DISA Network (DISANet) systems.

14. SUBJECT TERMS
Internet, Intranet, World Wide Web

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

3.10 DISAI 630-230-30, Electronic Mail Management, 6 November 1995.

3.11 Office of the Secretary of -Defense Memorandum, Instructions for Submitting Government Information Locator Service Records, 5 December 1995.

4. **Glossary and Definition of Terms.** A glossary and a list of definitions for terms used in this Instruction are provided at 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 DISA missions and personnel. Information services access and use by either Internet or Intranet is granted for conducting official business only (see reference 3.1). Such use will be monitored to ensure protection of networks and information and to verify compliance with these instructions. All DISA personnel may also be subject to unannounced computer inspections under the DISA Vulnerability Assessment and Analysis Program or other authority.

5.1 Content Sensitivity.

5.1.1 It is a known fact that criminal, foreign intelligence, and terrorist organizations actively monitor military and technical materials and discussions on the Internet and commercial OnLine service providers. While encouraged to post appropriate materials and documents to the Internet or Intranet, all DISA personnel must exercise extreme caution to ensure they discuss or post no 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.

5.1.2 All information posted to the Internet and/or Intranet will be reviewed and approved by the respective Deputy (Assistant Deputy) Director or Commander (Vice Commander) and by the DISA PAO, in accordance with para. 7, below, prior to release.

5.2 **Stewardship.** All DISA personnel and contractors have the inherent responsibility of "stewardship" and must continually promote the safe, effective, efficient, and legal use of all U.S. Government resources. DISA personnel must:

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

5.2.2 Maximize the use of existing Federal Government Internet servers and the-NIPRNet as the means to Internet access.

5.2.3 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, o-r others might-use to the disadvantage of DISA or to the U.S. Government. This information may include contractual, operationally sensitive,. or classified information.

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

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

5.3.1 Obtain or exchange information to support DOD or DISA missions.

5.3.2 Obtain or exchange information that enhances the professional skills of DISA employees and benefits the Agency and job performance within the Agency.

5.3.3 Improve professional or personal skills as part of a formal academic education or military or civilian professional development program (when approved by an immediate supervisor).

5.4 Incidental Use. Government computers may be used to access the Internet for incidental personal purposes such as brief communications, brief Internet searches, and other uses allowed by reference 3.2 as long as such use:

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

5.4.2 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.

5.4.3 Is of minimal frequency and duration and occurs during an employee's personal time.

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

5.4.5 Is not used for purposes that adversely reflect upon this Agency and the Federal Government. (A listing of prohibited uses of information services is at enclosure 2.)

6. **Information and the Internet.** Users may obtain or exchange

information using Internet host capabilities such as electronic mail (e-mail), WWW, file transfer protocol (FTP), or telecommunications-network (TELNET) services. This information may be categorized-as publicly releasable, limited release, or Privacy Act information.

6.1 Publicly Releasable Information. 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 DISA's mission, and consistent with the intent of the Freedom of Information Act. Publicly releasable information will be maintained and made available primarily through DISA's "external" WWW servers or, when appropriate, through other publicly accessible Internet hosts.

6.2 Limited Release. Limited release information includes DISA-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 include classified information only when appropriate system safeguards and certifications are in place (reference 3.3). Limited release information will not be made available to the general public. Limited release information made available to activities outside DISA must have appropriate user registration procedures, userid, and password controls.

6.3 Privacy Act Information. This 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 operation requirements mandate the use of Privacy Act information using the Internet or Intranet, it must be properly protected.

6.4 Release of Materials. Material proposed to be made available electronically to the publicly accessible Internet or the more restricted Intranet must be submitted through the same public affairs channels as "hard copy" material proposed for publication external to DISA or Internal to DISA, respectively.

7. **DISA Information Release and Review Authorities.** All information to be posted to a DISA Internet or Intranet host, whether for public or limited release, must undergo organizational and Agency-level reviews.

7.1 Reviews. All information must be reviewed and approved by the respective Deputy Director or Commander or Chief (or their authorized representatives) prior to posting to a DISA Internet or Intranet server. The proposed information must also be coordinated with and approved by the DISA Public Affairs Office (PAO) before it is released to the public or any audience outside DISA (see references **3.4, 3.5,** and **3.6).** Reviews must be redone when new information is made available or when the appropriate Deputy Director or Commander or designated representative determines that significant changes have been made in the content of the information previously posted to a

DISA Internet or Intranet server. DISA organizations are encouraged to coordinate with PAO to develop and streamline procedures for reviewing DISA WWW materials.-

7.2 Special Reviews. Deputy Directors and Commanders or Chiefs will coordinate the proposed information to be released with the DISA Regulatory General Counsel (RGC) and the Procurement and Logistics Directorate (D4) whenever the information to be posted poses potential legal or contracting consequences. When this review is considered necessary and is not documented, PAO will ensure the required coordination with RGC and D4 before approving the information for release.

8. **DISA Internet Services.** All DISA employees and contractor personnel will be given basic Internet access through the DISANet and DISA Internet services. Units with requirements extending beyond basic Internet service must comply with the following procedures:

8.1 Specialized Internet Services. DISA will not provide specialized network access or support services such as dial-in access or Integrated Services Digital Network (ISDN) connections unless deemed mission essential. Specialized services will be funded by the requesting organization or activity and must be processed through the Agency requirements identification process (references 3.7 and 3.8).

8.2 Internet and Intranet Servers and Connections. All DISA directorates and major field activities are encouraged to use existing DISA Internet and Intranet resources unless requirements clearly justify more equipment and services. All organizations or activities operating organizationally owned Internet and Intranet servers must also:

8.2.1 Comply with established DISA Internet and Intranet naming and addressing conventions for all internet host systems (reference 3.9). (Exceptions must be coordinated with and approved by the Commander, DISA Information Systems Center [DISC], and the Chief Information Officer [CIO].)

8.2.2 Obtain approval from the Commander, DISC, when servers require connections to the DISA-IS and its DISANet subcomponent.

8.2.3 Obtain the approval of the CIO prior to entering into any agreements with commercial Internet service providers.

8.2.4 Ensure that information systems security accreditation is requested in accordance with reference 3.3 before any Internet server becomes operational.

8.2.5 Ensure that appropriate personnel are identified and made available to the DISC local control center (LCC) to address operational problems stemming from the organization's web server or home page.

8.2.6 Ensure that all DISA Internet and Intranet servers comply with 24 X 7 operations. If any outage occurs, personnel will be called out during duty and nonduty hours- and-the server will be-restored as quickly as possible. Outage reporting information will be reported to the DISA LCC.

8.3 E-Mail and FTP Services.

8.3.1 E-Mail. All use of Agency e-mail must comply with the policies outlined in reference 3.10. All personnel must ensure that the content of their e-mail messages is professional and does not misrepresent or misstate Agency or DOD positions or policies.

8.3.2 **File Transfers.** DISA personnel will not download commercial software or "shareware" that obligates the Government for payment. All users must ensure that downloaded software is properly screened and cleared of viruses before storing software on DISA network resources. (Virus detection software is available under DISANet "Utilities.") Users must also be aware of network disk storage limitations and consider such limitations before storing files or data on network resources.

8.3.2.1 Shareware like commercial software may be purchased and used when properly obtained through established Agency acquisition processes (references 3.7 and 3.8).

8.3.2.2 Obtaining executable software from FTP sites outside DOD and other governmental agencies is discouraged.

8.4 **Internet Chat and Phone Capabilities.** All Internet users must exercise caution when using these services and must comply with the policies outlined in this document. All plans to use Internet phone services must first be processed and approved through the Agency requirements process as outlined in reference 3.7.

9. **DISA World Wide Web (DISA WWW).** The DISA WWW will be the primary means DISA uses to share information with the general public. As such, all DISA organizations and activities using these resources must comply with the following operational procedures developed by CIO and DISC.

9.1 **Web Home Page Designs.** All web pages within the DISA WWW system will be considered official and must conform to established page design and performance standards (found at URL http://www.disa.mil/info/disawww.html). DISA organizations and activities may obtain web page design and management assistance from DISC through the DISA Webmaster. All DISA directorates and "major" field activities that deveiop web pages must ensure that the information provided is professional, accurate, and maintained on an ongoing basis.

9.2 Web Responsibility. All information presented on the DISA WWW is the direct responsibility of the senior management within each DISA

directorate or activity who sponsors the web page. These persons must ensure that all information is kept current and that all DISA WWW resources which are no longer-required are properly released.

9.3 **Government Information Locator Services (GILS).** All originators of publicly released information dissemination products within DOD must ensure GILS records are created and, when appropriate, updated (reference 3.11). The DISA Webmaster will meet this reporting requirement and provide the information required once the available information has properly been cleared through proper review and approval authorities.

10. DISA Internet Working Group. The DISA Internet Working Group will serve as the Agency-wide forum to address issues relating to the provision and use of Intranet and Internet servers. This group will be chaired by a person appointed by the Commander, DISC; its membership will consist of representatives from DISA organizations or activities who operate Internet and Intranet services. This group will coordinate its actions with the Commander, DISC '(operations and maintenance issues) and the CIO (policy, acquisition, business planning, and information systems security issues).

11. Procedures.

11.1 **Internet** Access, Server, **and Other Special Internet Services.** All requests for Internet and Intranet access and service requirements must be submitted using procedures outlined in reference 3.7.

11.2 **Approval Process of DISA Web Pages.** All DISA web pages will be developed using the following procedures:

11.2.1 **Organizational Approval.** All information to be presented on a DISA web page must be approved by a Deputy Director or Commander or Chief or their designated representatives). 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 DISA Webmaster. (Information which has previously been approved by organizational authorities and the PAO for public or external distribution need not be resubmitted for approval for publishing on a World Wide Web server.)

11.2.2 **Agency Approval.** Once the organizational information is approved and assembled, it is forwarded to the DISA PAO for approval when information is slated for public release or release to activities outside DISA (see references 3.4 and 3.5). (Information which has previously been approved by the DISA PAO for public or external distribution need not 'be resubmitted for approval for publishing on a World Wide Web server.j Once approved by PAO, the planned information release and web pages are forwarded by PAO to either:

11.2.2.1 The DISA Webmaster for DISC-provided web services and

postings.

11.2.2.2 The submitting organization when the information and web pages are to be posted to an organizational server.

11.3 Security Accreditation. Security accreditations must be accomplished for all Internet and Intranet hosts (to include all DISA WWW servers) and web pages. Security accreditation must be requested from the CIO using the procedures described in reference 3.3.

11.4 Operational Approval. All DISA Internet and Intranet hosts that interface with or connect to the DISANet must be reviewed by the Commander, DISC. Requests for this service should be submitted to the Commander, DISC, through the Agency requirements process outlined in reference 3.7.

12. Responsibilities.

12.1 Chief Information Officer (CIO). The CIO will:

12.1.1 Develop Agency policy regarding the use of the Internet and Intranet.

12.1.2 Coordinate the effective use of security-related resources to include the development and promulgation of cost-effective approaches to securing information technology and for providing centralized INFOSEC enforcement and oversight of all DISA information systems including those interfacing with the internet and intranet.

12.1.3 Incorporate DISA Internet and Intranet plans and infrastructure requiremerits into the DISA-IS architecture.

12.1.4 Develop appropriate Agency standards for products and services to be used with DISA Internet, Intranet, and associated information services.

12.1.5 Issue statements of accreditation after requirements for security accreditation have been met in accordance with reference 3.3.

12.2 **Commander, DISA Information Systems Center (DISC).** The Commander, DISC, will:

12.2.1 Manage, plan, budget, maintain, and operate the DISA Intranet system, the DISA WWW and Internet system, and the DISA WWW Internet infrastructures.

12.2.2 Appoint the DISA Webmaster and develop the appropriate technical support staff required to provide DISA enterprise-wide Internet and Intranet services.

12.2.3 Develop operations and maintenance policies and supporting procedures required for the DISA WWW and its enterprise-level infrastructure.

12.2.4 Through the DISA Webmaster, develop standards and policies appropriate for information presented to the public on the DISA WWW or publicly available Internet hosts and include GILS reporting for DISA WWW information sources.

12.2.5 Establish appropriate auditing and control processes and procedures to ensure the efficient and effective use of the Internet and Intranet.

12.2.6 Develop, staff, and operate an Agency-level program to train DISA organizational web masters and "web page" editors.

12.2.7 Integrate functional applications planned for the DISA-IS and DISA Internet and Intranet infrastructures.

12.2.8 Manage the Internet and Intranet services and servers. (Management will be in accordance with the directives of the Technical Architecture Framework for Information Management [TAFIM] and Global Control Concept documents. Management of the health and welfare of both the base operating system and supported applications wili be handled by the Simple Network Management Protocol [SNMP], wherever possible.)

12.3 Chief, DISA Security (D16). The Chief , D16, will, in conjunction with CIO, investigate crimes and security violations (outside the purview of the DISA Inspector General) regarding DISA personnel and their use of the Internet and/or Intranet.

12.4 **Commander, Joint Interoperability and Engineering Organization (JIEO)** . The Commander, JIEO, will:

12.4.1 Provide required interoperability engineering support to ensure the DISA Internet infrastructure complies with appropriate DOD and industry standards.

12.4.2 Help develop DISA Internet standards to ensure DISA's compliance with appropriate Defense Information Infrastructure, Common Operating Environment, and Shared Data Environment standards.

12.5 **Deputy Directors, Headquarters, DISA; Commanders and Chiefs of DISA Field Activities; and the Deputy Manager, NCS.** These individuals wili:

12.5.1 Appoint organizational web masters and web page editors to manage organizational web servers and oversee the design and maintenance of organizational web pages.

12.5.2 Serve as the organizational approval authority for information that is to be released to DISA Internet hosts to include DISA WWW servers.

12.5.3 Appoint organizational representatives to the DISA Internet

Working Group when organizations operate or use Internet hosts or web pages as a means to distribute information.

12.5.4 Ensure that information provided on any of their organizational information servers connected to the Internet and/or Intranet does not contain classified, unclassified sensitive, or Privacy information, or information that could enable the recipient to infer classified or unclassified sensitive information, either from individual segments of the information, or from the aggregate of all the information available.

12.6 Chief, DISA Public Affairs. The Chief, PAO, serves as the Agency information release approval authority for all DISA Internet information in accordance with references 3.4, 3.5, and 3f.

12.7 Deputy Director for Operations, D3. The Deputy Director of Operations, through the Global Operations and Security Center (GOSC), will:

12.7.1 Work with the NSA to resolve any risk assessments identified to DISA invoiving DISA-Internal Security and DoD Policy within the GOSC realm (including approved Vulnerability Assessment and Analysis Programs (VAAPs) of DISA web sites).

12.7.2 Provide professionai guidance and referral, relevant to the content of information released on external domains.

12.8 Program Director, **INFOSEC Program Management Office (D25).**

12.8.1 Provide information systems security certification and security testing to ensure that user access to DISA external web servers is isolated from DISANet, other DISA networks, and internal LANs.

12.8.2 In coordination with the CIO, periodically assess the effectiveness of web server security controls implemented.

13. **Use of DISA Internet, Intranet, and World Wide Web by DISA Personnel..** All DISA personnel are responsible for promoting the effective and efficient use of the DISA Internet, Intranet, and WWW services. All DISA personnel should:

13.1 Ensure that all information provided to DISA Internet and Intranet hosts reflects the highest standards of quality and utility.

13.2 Report all suspected intrusions or compromises of DISA Internet or Intranet services, controls, or any suspected alterations of the information DISA makes available on its Internet hosts. Direct these reports to the Commander, DISC, or to the DISA Webmaster and staff.

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

14. Policy **Changes.** All servicing civilian personnel offices must be notified of any changes to this policy well in advance of its implementation to ensure DISA's bargaining obligations are effectively met in the collective bargaining process.

FOR THE DIRECTOR, DISA, AND MANAGER, NCS:

A. FRANK WHITEHEAD
Colonel, USA
Chief of Staff

2 Enclosures:
1 Glossary and Definitions
2 Prohibited Uses of Internet Services

*This Instruction cancels D?L 95-13, 14 September 1995
OPR: CIO
DISTRIBUTION: Y

Return to:
Beginning of DISAI 630-225-7
Publication Listing
DISA Home Page

Sharon B. Willard, *willards@ncr.disa.mil* - Last revision: 6 Sep 96

Enclosure 1: DISAI 630-225-7

Glossary and Definitions

Acronyms and Abbreviations

CIO	Chief Information Officer
DISA	Defense Information Systems Agency
DISAI	Defense Information Systems Agency
DISA-IS	DISA Information System
DISC	DISA Information Systems Center
DISANet	DISA Network
DOD	Department of Defense
e-mail	Electronic Mail
FOUO	For Official Use Only
FTP	File Transfer Protocol
GILS	Government Information Locator Services
GOSC	Global Operations and Security Center
HTTP	Hypertext Transfer Protocol
INFOSEC	Information Security
ISDN	Integrated Services Digital Network
JIEO	Joint Interoperability and Engineering Organization
LCC	Local Control Center
NIPRNet	Non-secret Internet Protocol Network
OMNCS	Office of the Manager, National Communications System
PAO	Public Affairs Office
RGC	Regulatory General Counsel
SNMP	Simple Network Management Protocol
TAFIM	Technical Architecture and Framework for Information Management
URL	Uniform Resource Locator
VAAP	Vulnerability Assessment and Analysis Program/td>
w w w	World Wide Web

Definitions

Basic Internet Services. In this publication, Internet services refer to the general Internet capabilities provided to the typical DISA -- user. These services are provided within estab-lished DISA Network (DISANet) resources and typically include a web browser, access to FTP and telnet services, and e-mail capabilities to Internet and Intranet addressees. Internet services are predominantly user-level services.

Browser. A computer application that allows a user to view information on the World Wide Web. At a minimum, browsers are able to display information they receive in the hypertext markup language.

DISA **Internet.** Refers to interconnection of DISA-owned and DISA-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 DISA-owned systems with other non-DISA networks.

DISA Intranet. Refers to DISA-owned and DISA-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 DISA, its components, or its contractors.

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

External Server. An Internet host computer system which 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 transfers of files between Internet users and systems.

Government Information Locator Service (GILS). A card catalog-like system that identifies public information resources throughout the Federal Government, describes information avail-able in these resources, and provides assistance in obtaining the information.

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.

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 academia, business, government, and personal interests.

Internet Chat. Systems that allow users to exchange text

Enclosure 2: DISAI 630-225-7

PROHIBITED USE OF INTERNET SERVICES

1. The use of Internet services in the following types of activities is specifically prohibited.

1.1 Illegal, fraudulent, or malicious activities.

1.2 Partisan political activity, political or religious lobbying or advocacy, or activities on behalf of organizations having no affiliation with DISA or DOD.

1.3 Activities whose purposes are for personal or commercial financial gain. These activities may include chain letters, solicitation of business or services, sales of personal property.

1.4 Unauthorized fundraising or similar activities, whether for commercial, personal, or charitable purposes. Official morale, welfare, recreation, officer, and enlisted aid activities are authorized.

1.5 Accessing, storing, processing, displaying, or distributing offensive or obscene material such as pornography and hate literature.

1.6 Storing, processing, or distributing classified, proprietary, or other sensitive or for official use only (FOUO) information on a computer or network not explicitly approved for such processing, storage, or distribution.

1.7 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.

1.8 Using another person's account or identity without his or her explicit permission, e.g., by forging e-mail.

1.9 Viewing, damaging, or deleting files or communications belonging to others without appropriate authorization or permission.

1.10 Attempting to circumvent or defeat security or auditing systems without prior authorization and other than as part of legitimate system testing or security research.

1.11 Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

1.12 Permitting any unauthorized person to access a DISA- or DOD-owned system.

1.13 Modifying-or altering the operating system or system configuration without first obtaining permission from the owner or administrator of that system.

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

Return to:
Publication Listing
DISA Home Paae

Sharon B. Willard, willards@ncr.disa.mil - Last revision: 6 Sep 96

siprnet New Search options - help

Other Search Engines

Alta Vista - WebCrawler - HotBot - Lycos - Infoseek - Excite -- Image Surfer - DejaNews - More...

Yellow Pages - People Search - City Maps - Get Local - Today's Web Events & Chats - More Yahoos