STATE OF NEW YORK
EXECUTIVE DEPARTMENT
DIVISION OF MILITARY AND NAVAL AFFAIRS
330 Old Niskayuna Road
Latham, New York 12110-2224

DMNA Regulation
Number 25-33 **12 December 1997**

Information Management: Computer Networks

INTERNET/INTRANET ACCESS AND ELECTRONIC MAIL

Summary. This regulation covers the current DMNA policy for access to the Global Internet (World Wide Web), Intranets and other Local or Wide Area Networks, and Electronic Mail (E-mail) use.

Applicability. This regulation applies to all components of the New York State Division of Military and Naval Affairs, consisting of: The headquarters staff located primarily in Latham, the State Emergency Management Office (SEMO), and elements of the organized militia; New York Army National Guard (NYARNG), New York Air National Guard (NYANG), New York Guard (NYG), and the New York Naval Militia (NYNM).

Proponent and Exceptions. The proponent of this regulation is the Directorate of Communications and Information Management.

Supplementation. Supplementation of this regulation and establishment of command and/or local policies particular to the major commands is encouraged.

Interim Changes. Interim changes or additions are not official unless authenticated by the Assistant Adjutant General. Users will ensure changes are provided to DMNA, ATTN: MNCM-AS for inclusion in updates.

Changes to Regulation. Changes or corrections will be reported promptly directly to The Adjutant General, Division of Military and Naval Affairs, ATTN: MNCM-AS, 330 Old Niskayuna Road, Latham, NY 12110-2224. Or, phone (518) 786-4970, DSN 489-4970. Facsimile is (518) 786-4785, or DSN 489-4785, ATTN: MNCM-AS.

Distribution. Distribution of this publication is made to ensure consistent Internet /Intranet, and Electronic Mail usage throughout elements of the Division of Military and Naval Affairs.

Contents

Chapter 1
Introduction

1-1. Purpose.

a. The connection to the global Internet or an Intranet exists to facilitate the official work of the Division of Military and Naval Affairs (DMNA). The Internet or Intranet facilities and services will contribute broadly to the missions of DMNA.

b. The Internet or Intranet connection and services are provided for employees and persons legitimately affiliated with DMNA for the efficient exchange of information and the completion of assigned responsibilities consistent with DMNA's statutory purposes.

c. The use of the Internet or Intranet facilities by any employee or other person authorized by the department must be consistent with this Acceptable Use Policy, security policies, and applicable DOD policies and regulations.

d. Access to the Internet through the use of government equipment and communications lines is for official use only, except for authorized personal (non-official) use. As stated in DOD Directive 5200.28, DDN communication systems are for use by government agencies, their employees, and authorized contractor personnel for the conduct of official DOD business only. AR 25-11, AFI 33-129, and Navy Message ALCOM 035/95 define official messages as those that specifically pertain to the official functions of the military establishment. **DoD Directive 5500.7-R, Joint ethics Regulation (JFR), authorizes personal incidental use as described later.**

1-2. References. Required and related publications are listed in Appendix A.

1-3. Explanation of abbreviations and terms. Abbreviations and special terms used in this regulation are explained in the glossary.

1-4. Responsibilities and Rights.

a. Agency executive management will ensure that policies are implemented by program unit management and unit supervisors.

b. The Directorate of Communications and Information Management (MNCM) is the functional proponent for Internet, Intranet, and E-mail policy and procedures.

c. Directorates and MACOMs will develop and/or publicize record keeping practices in their area of responsibility including the routing, format, and filing of records communicated via E-mail. They will train staff in appropriate use and be responsible for ensuring the security of physical devices, passwords, and proper usage.

d. Network administrators and internal control (and/or internal audit) staff are responsible for E-mail security, backup, and disaster recovery.

e. WebMaster. The Website/Document Point of Contact ("WebMaster") will -- (per HQ DA Guidance 30 Oct. 96; Guidance for the Management of Army Websites, and AFI 33-129, Transmission of Information via the Internet, para 4 Web Administration):

(1) Ensure that information published on the website is accurate, timely, represents the official army/ air/ DMNA position, and is properly cleared for public dissemination.

(a) Agency Business Process.

(b) Editorial Controls.

(c) Links.

(d) Stable and Reliable.

(e) Technology.

(2) Ensure appropriate security and access controls are in place, commensurate with the perceived threats, and to ensure that information which is classified, unclassified but sensitive, information which cannot be disclosed under the privacy act, for Official Use Only (FOUO), or Freedom of Information Act (FOIA) - exempt information (such as draft policies and regulations, or pre-decisional information) is not made available to unauthorized individuals or organizations.

(3) Provide the highest possible level of assurance that information made available or received from the public does not contain malicious software code such as viruses, Trojan horses, logic bombs, bacteria and worms, or if it does, to sufficiently notify the user before the download of such information begins.

(4) Respond to customer or user E-mail and direct queries or requests for information to the responsible party within the organization.

(5) Ensure that the organizations website provides point of contact information,

(6) Policy Research State and Federal Internet policies and develop and maintain a DMNA Regulation on same.

f. All users will:

(1) Act with responsibility and respect.

(a) Be courteous and follow accepted standards of etiquette.

(b) Protect others' privacy and confidentiality.

(2) Knowledge of the Internet/Intranet. The user agrees to obtain a basic knowledge of the Internet/Intranet, its operating principles and procedures.

(3) Validate Information. Consider organizational access before sending, filing, or destroying E-mail messages.

(4) Security. Protect their passwords.

(5) Housekeeping. Remove personal messages, transient records, and reference copies in a timely manner.

(6) Avoidance of Improper Use. Avoid violation of certain generally accepted guidelines on Internet/ Intranet usage such as restrictions on mass mailings, mass advertisements, pirating or copying software, mail bombing or other methods to deny service or access to other users, and attempts to violate security.

(7) Compliance with Laws. The user will ensure that its use of the Internet/Intranet complies with all applicable federal, state and local laws and regulations, including but not limited to those practices of law which protect against compromise of copyrights, trade secrets, proprietary information and other intellectual copyrights, libel or defamation of character, invasion of privacy, tortuous interference, and export of technical or military data to prohibited countries.

(8) Compliance with military, agency and unit regulations, policies, directives, procedures, and standards.

g. *DMNA (and other network operators) Rights.*

(1) Pursuant to the Electronic Communications Privacy Act of 1986 (18 USC 2510 et seq.), notice is hereby given that there are **no** facilities provided by this system for sending or receiving private or confidential electronic communications. System administrators have access to all mail and user access requests, and will monitor messages as necessary to assure efficient performance and appropriate use. Messages relating to or in support of illegal activities will be reported to the appropriate authorities.

(2) Network Administrators reserve the right to log network use and monitor file server space utilization by users on DMNA's Intranet, and assumes no responsibility or liability for files deleted due to violation of file maintenance procedures or time limitations.

(3) Network Administrators reserve the right to monitor Internet access by users, and to inquire of the user's supervisor if such access if for official use only when usage is inconsistent with the individual's duty position.

(4) Network Administrators reserve the right to remove a user account from the network.

(5) Use of any information obtained is at the user's risk. Any computer connected to a network must have anti-virus software installed.

(6) Network Administrators reserve the right to change its policies and rules at any time. Network Administrators make no warranties (expressed or implied) with respect to Internet/Intranet service, and it specifically assumes no responsibilities for:

(a) Any costs, liabilities or damages caused by the way the user chooses to use his/her agency Internet/Intranet access.

(b) Any consequences of service interruptions or changes, even if these disruptions arise from circumstances under the control of the Network Administrators. Internet/Intranet services are provided on an as is, as available basis.

THIS

PAGE

INTENTIONALLY

LEFT

BLANK

Chapter 2
Internet / Intranet Access

2-1. Principles of Acceptable Use.

a. Internet/Intranet users are required:

(1) Respect the privacy of other users; for example, users shall not intentionally seek information on, obtain copies of, or modify files or data, belonging to other users, unless explicit permission to do so has been obtained.

(2) Obtain a basic knowledge of the Internet/Intranet, its operating principles and procedures.

(3) Respect the legal protection provided to programs and data by copyright and license.

(4) Protect data from unauthorized use or disclosure as required by state and federal laws, DMNA and DOD regulations.

(5) Respect the integrity of computing systems. For example, users shall not use or develop programs that harass other users or infiltrate a computer or computing system and/or damage or alter the software components of a computer or computing system.

(6) Be aware of the classification of any information contained in data files or correspondence which is being transported using Internet/Intranet access, and not to exchange information in un-encrypted form which is private or confidential. THE Internet/Intranet IS NOT SECURE AND CLASSIFIED INFORMATION WILL NOT BE TRANSMITTED IN ANY FORMAT. Under no circumstances should data ever be transmitted, which if intercepted, would place DMNA in violation of any law.

b. The content of anything transmitted over the Internet/Intranet (regardless of its state of encryption) must be appropriate and consistent with DMNA and DOD policy, and is subject to the same restrictions as other correspondence.

c. Validation of Information - The user is responsible for validating the integrity of the information and data received or transmitted over the Internet/Intranet. Any receipt of images or programs over the Internet/Intranet must be checked with an anti-virus program before executing or distributing them.

2-2. Acceptable Use. Federal and state government communication systems and resources shall be for official use only, except for authorized personal (nonofficial) use. Federal and state government communication systems include government owned electronic mail, Internet and Intranet systems, and commercial systems when use is paid for by the government. Federal and state government resources include equipment, personnel, and property (e.g., computers, facilities, etc.).

a. Official use includes communications and research on the Internet that is necessary in the interest of the federal or state government as well as emergency communications. Upon approval, official use will be extended to government employees deployed away from home for an extended period of time on official business.

b. Authorized personal use includes incidental use as authorized by this regulation or as specifically authorized by supervisors using guidelines contained herein. Authorized incidental use includes briefly searching the Internet under the following conditions:

(1) You have permission to use your computers to access Internet resources for professional development purposes, subject to ensuring that your primary dutues and mission are accomplished. Professional development includes Internet usage related to college or military academic courses.

(2) You also have permission to use your computer to access Internet resources for any other personal reason; but may do so only before and after work hours, or during your lunch period or other authorized break

during the work day. Personal use must still comply with responsibilities outlined in paragraph 1-4.f. and principles of acceptable use in paragraph 2-1.

2-3. Unacceptable Use. Accessing the Internet through a government computer or network uses a government resource. Government-provided hardware and software are for conducting official and authorized government business. This does not prohibit commanders from authorizing personnel to use government resources to further their professional and military knowledge if they determine it is in the best interest of the government and authorization is documented by letter, local operating instruction, or explicit policy. Using the Internet for other than authorized purposes may result in adverse administrative or disciplinary action. The following activities involving the use of government-provided computer hardware or software listed in paragraphs *a.* through *q.* are specifically prohibited:

a. For activities unrelated to DMNA's (state) or DOD's (federal) official and authorized government business or mission, other than authorized personal use.

b. For activities unrelated to official assignments and/or job responsibilities, other than authorized personal use.

c. Illegal, fraudulent, or malicious activities.

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

e. 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.

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

g. Accessing, storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material. Offensive material includes, but is not limited to, "hate literature," such as racist literature, materials or symbols (for example, swastikas, neo-nazi materials, etc.), and sexually harassing materials. Obscene material includes, but is not limited to, pornography and other sexually explicit materials.

h. 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.

I. 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.

j. Using another person's account or identity without their explicit permission, e.g., by forging E-mail.

k. Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.

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

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

n. Permitting any unauthorized person to access a DMNA- or DOD-owned system.

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

p. Storing or processing copyrighted material (including cartoons) unless approval is obtained from author or publisher.

q. Participating in "chat lines" or open forum discussion unless for official purposes and after approval by appropriate Public Affairs channels.

2-4. Computer Resources. DMNA endorses the following guidelines concerning computing resources;

a. Respect the network as a shared resource. Be sensitive to the impact of your traffic on network performance. This means not abusing mailing lists, not bringing large files across the network, etc.

b. The distribution of programs, databases, and other electronic information resources are controlled by the laws of copyright, licensing agreements, and trade secret laws. These will be observed.

2-5. Information Dissemination.

a. All information published, disseminated or otherwise made available via the Internet or Intranet must comply with all applicable statutes, regulations and policies.

b. Information for the DMNA Website, which is forwarded to the DMNA WebMaster for posting, must be approved by the Director or MACOM commander or their designated representative.

c. Links on the DMNA Website to unit's homepages must be approved by the MACOM chain-of-command. Such linkage may be construed as lending an "official" status to these sites and care should be given to ensure they are not contrary to policy.

d. DOD personnel, while acting in a private capacity and not in connection with their official duties, have the right to prepare information for public release through non-DOD forums or media. Such activity is authorized if no laws or regulations are violated, ethical standards are maintained, the preparation is not done during duty hours or utilizing governmental facilities or equipment, and the author does not release official governmental information not available to the public (see DoDD 5230.9, 9 Apr. 96).

2-6. Enforcement and Violations.

a. This policy is intended to be illustrative of the range of acceptable and unacceptable uses of the Internet/Intranet facilities and is not necessarily exhaustive. Questions about specific uses related to security issues not enumerated in this policy statement and reports of specific unacceptable uses must be directed to MNCM. Other questions about appropriate use must be directed to your supervisor.

b. DMNA MNCM will review alleged violations of the Internet/Intranet Acceptable Use Policy on a case-by-case basis. Clear violations of the policy which are not promptly remedied will result in termination of Internet/Intranet services for the person(s) at fault, and referral for disciplinary actions as appropriate.

c. Improper use or activities by uniformed members may result in administrative or other disciplinary action such as actions mandated by the Uniform Code of Military Justice (Article 92 UCMJ), or the NYS Military Law, non-judicial punishments, performance appraisals, and personnel disciplinary actions.

THIS

PAGE

INTENTIONALLY

LEFT

BLANK

Chapter 3
E-mail Usage

3-1. Use of E-mail.

a. Official use. E-mail services, like other means of communication, are to be used to support agency business. Staff may use E-mail to communicate informally with others in the agency so long as the communication meets professional standards of conduct. Staff may use E-mail to communicate outside of the agency when such communications are related to legitimate business activities and are within their job assignments or responsibilities.

b. Illegal use. Staff **will not** use E-mail for illegal, disruptive, unethical or unprofessional activities, or for personal gain, or for any purpose that would jeopardize the legitimate interests of New York State.

c. Authorized personal use. Personal E-mail communications, not involving long distance charges, made from the employee's usual work place that are most reasonably made during working hours such as:

(1) E-mailing short messages to relatives, friends, and fellow employees.

(2) Receiving E-mail as long as comparable receipt would be acceptable via telephone and the use is no more disruptive that a telephone call, are authorized.

3-2. Privacy and Access.

a. E-mail messages are **not** personal and private. E-mail system administrators will **not** routinely monitor individual staff member's E-mail and will take reasonable precautions to protect the privacy of E-mail. However, program managers and technical staff may access an employee's E-mail:

(1) For a legitimate business purpose (e.g., the need to access information when an employee is absent for an extended period of time).

(2) To diagnose and resolve technical problems involving system hardware, software, or communications.

(3) To investigate possible misuse of E-mail when a reasonable suspicion of abuse exists or in conjunction with an approved investigation.

b. A staff member is prohibited from accessing another user's E-mail without his or her permission.

c. E-mail messages sent or received in conjunction with agency business may:

(1) Be releasable to the public under the Freedom of Information Law.

(2) Require special measures to comply with the Personal Privacy Protection Law.

d. **All** E-mail messages **including personal communications** may be subject to discovery proceedings in legal actions.

3-3. Management and Retention of E-mail Communications.

a. Applicable to all E-mail messages and attachments. Since E-mail is a communications system, messages will not be retained for extended periods of time. Users must remove all E-mail communications (empty their trash) in a timely fashion. If a user needs to retain information in an E-mail message for an extended period, they will transfer it from the E-mail system to an appropriate electronic or other filing system. E-mail administrators are authorized to remove any information retained in an E-mail system that is more than **180 days** old.

b. Applicable to records communicated via E-mail. E-mail created in the normal course of official business and retained as evidence of official policies, actions, decisions or transactions are records subject to records management requirements under the NYS Arts and Cultural Affairs Law and specific program requirements.

c. Examples of messages sent by E-mail that typically are records include:

(1) Policies and directives.

(2) Correspondence or memoranda related to official business.

(3) Work schedules and assignments.

(4) Agendas and minutes of meetings.

(5) Drafts of documents that are circulated for comment or approval.

(6) Any document that initiates, authorizes, or completes a business transaction.

(7) Final reports or recommendations.

d. Some examples of messages that typically do not constitute records are:

(1) Personal messages and announcements.

(2) Copies or extracts of documents distributed for convenience or reference.

(3) Phone message slips.

(4) Announcements of social events.

3-4. Records.

a. Records communicated using E-mail need to be identified, managed, protected, and retained as long as they are needed to meet operational, legal, audit, research or other requirements. Records needed to support program functions must be retained, managed, and accessible in existing filing system outside the E-mail system in accordance with the appropriate program unit's standard practices.

b. Records communicated via E-mail will be disposed in accordance with the applicable record keeping system. Program managers will consult with the Agency Records Management Officer [MNCM-AS] concerning RDAs applicable to their program's records.

(1) State. A Records Disposition Authorization (RDA) approved by State Archives and Records Administration (SARA).

(2) Army. AR 25-400-2, *The Modern Army Record keeping System (MARKS).*

(3) Air Force. AFMAN 37-123, *Management of Records;* AFI 37-138, *Records Disposition -- Procedures and Responsibilities*; and AFMAN 37-139.

c. Users will:

(1) Dispose of copies of records in the E-mail system after they have been copied and filed in a record keeping (archival) system. If electronic archival files are not maintained hard copies should be placed in the functional files;

(2) Delete records of transitory or little value that are not normally retained in record keeping systems as evidence of agency activity.

Chapter 4
Security

4-1. System Security Considerations. Because the Internet is a public network, information placed on the Internet without access controls is available to everyone. Using access controls effectively reduces the risk of accessing information on the Internet. Protecting the confidentiality, integrity, and availability of information resources is a priority for all employees at all levels of DMNA.

4-2. Internet Controls.

a. Access. All Internet/Intranet access must be approved and authorized by the appropriate director/commander. Restricting access to information is only part of the security equation.

b. Authentication. Network Administrators will require the appropriate authentication for anyone accessing their local Intranet. The Internet is an inherently unsecured network. Information packets traveling across the Internet jump from node to node to travel from origin to destination. At any point along the way, interception of the information can occur. To prevent unauthorized disclosure of information, security controls must be implemented. Therefore, to fully protect information resources, it takes a combination of access and security controls.

4-3. Internet Threats. Internet access growth, coupled with the increase of information stored, processed, or transmitted on DMNA or DoD computer systems increase the threat and vulnerability of DMNA or DoD information resources. Network attacks from the Internet primarily come in two forms--structured and unstructured.

a. Structured attacks are sophisticated and organized, and are the most severe threat to our systems and our information resource. Structured attacks come from groups of individuals who have common goals. These groups target specific systems or groups of systems for industrial and military espionage, malicious intentions, financial gains, and, or military operational advantage.

b. Unstructured attacks are less organized but usually employ the same techniques as structured attacks. For example, the common computer "hacker" is an unstructured attacker. These attackers pick their targets at random, probing different domains in search of common system vulnerabilities to exploit. Individual attackers infiltrate systems out of curiosity to boast their success in the hacker community, enabling them to achieve a higher status. They may, however, have malicious intentions (for example, implanting logic bombs, Trojan horses, denial of service attacks, or altering data) just to cause grief to the system's legitimate users.

4-4. Countering the Threat. The skill and knowledge levels of the systems administrator, in concert with the applied technical solutions or "patches" available, are the key determinants in keeping a system and its information secure. In a web environment, the information providers are also key because they identify the value of the information and the type of access controls and techniques necessary to protect information from unauthorized disclosure. Systems administrators, information providers, and page OPRs must maintain a awareness of the ever changing threat to information and systems, and to report any unusual activity on a system. Listed below are some of the common techniques used to attack a system or its information:

a. IP Spoofing. Potential intruders attempt to gain access to a system or its information by creating packets with spoofed (faked) source IP addresses. This exploits applications that use authentication-based IP addresses and leads to unauthorized user access, and possibly "root access" (the ability to control an entire computer system, even to the exclusion of the system owner).

b. Packet Sniffers. Information traverses the Internet in packets through a series of computers. These computers (routers, bridges) reside at any given point on the Internet, and are most likely outside of state or DoD control. These computers are also vulnerable to the same computer threats as state or DoD systems, and an intruder may compromise them by gaining root access. Once an intruder has gained access, they can activate a program (such as a Trojan horse) to collect information traversing the computer (for example, Internet domain,

account names, IDs, and passwords). Generally, good password administration and encryption techniques can thwart this threat.

(1) Trojan Horse. These are hidden computer viruses or viruses in disguise. Trojan horses are often computer programs embedded in other programs or software. This is done by the intruder so the user is unaware of the Trojan horse's presence or existence. Trojan horse programs do something the programmer intended but that the user would not approve of if they knew about it. A virus is a particular case of a Trojan horse that is able to spread to other programs. Some Trojan horses hide in a system and capture information (for example, IDs and passwords of legitimate users) so the programmer can return to the system at a later time to damage, destroy, or steal data. In the case of an ID/password capture or compromise, an intruder gains the capability of entering the system as a legitimate user.

(2) Network Monitoring Attacks. Systems at risk are systems that offer remote access through remote login, TELNET, and FTP. This threat involves a monitoring tool that uses a promiscuous mode of a specific network interface to capture host and user authentication information on all newly opened FTP, TELNET, and remote sessions. Intruders typically install Trojan horse programs to support subsequent access to the compromised system and to hide their network monitoring process. This technique threatens all user account and password information derived from FTP, TELNET, and remote sessions passing through the same network as the compromised system.

4-5. Downloading Files from the Internet. To protect against downloading viruses, users must virus-check all downloaded files. This applies to sound and video files as well as files attached to E-mail messages. If possible, download files to a floppy disk and virus-check them before placing them on the computer's hard drive. If files are compressed, perform a second check of the decompressed files. To prevent the possibility of rapidly spreading a virus, do not download files to a network or shared drive. DMNA allows the use of public domain or shareware software only after it is certified by a software testing facility.

4-6. IDs and Password Protection.

a. Transmission Protection. The Internet is an unsecured network where compromise of a user ID and password can occur during open transmission. Do not transmit user IDs and passwords without encryption. Secure sockets layer (SSL) protocol provides a transmission level of encryption between the client and server machines. In addition to encryption protections for passwords, use one time password systems to ensure password integrity.

b. Changing. To safeguard their accounts and passwords, any user changes of passwords must follow published guidelines for good passwords. Accounts and passwords are normally assigned to singe users and are not to be shared with other persons without authorization. Users are expected to report any observations of attempted security violations.

4-7. E-mail.

a. DoD DOES NOT consider E-mail via multi-channel Memorandum Distribution Facility)MMDF) on the Internet as an Official message transport media. The future Defense Message System (DMS) will be implemented as the official message transport media.

b. E-mail security is a joint responsibility of agency technical staff and E-mail users. Users must take all reasonable precautions, including safeguarding and changing passwords, to prevent the use of account by unauthorized individuals.

4-8. OPSEC. The Internet access available to personnel at home and at work is an additional security factor. OPSEC training and education apply to computer use just as it does in conversations between personnel, correspondence, and telephone conversations. Policies against communicating with unauthorized personnel also apply to Internet communications. News groups (Network News Transfer Protocol [NNTP], Usenet News, Chats, etc.) give personnel the opportunity to converse electronically to a worldwide audience. Military and government employees will refrain from discussing work-related issues in such open forums. Such discussions could result in unauthorized disclosure of military information to foreign individuals, governments, or intelligence agencies or the disclosure of potential acquisition sensitive information. For example, news media monitoring the Internet may construe an individual's "chat" as an official statement or news release.

Appendix A - References

Section I
Required Publications

1-1. New York State Policies (http://www.irm.state.ny.us).

a. Governor's Task Force on Information Resource Management, Technology Policy 96-8, subject: NYS Use of the Internet, 3 May 96.

b. Governor's Task Force on Information Resource Management, Technology Policy 96-14, subject: NYS Use of Electronic Mail, 11 June 96.

1-2. Department of Defense (http://www.dtic.mil/defenselink/about.html).

a. Deputy Sec of Defense, Memorandum 17 Feb 95, subject, Clearance Procedures for Making Electronic Information Available to the Public (http://www.dtic.mil/defenselink/memo.html).

b. DoDD 5230.9, 9 April 96, subject: Clearance of DoD Information for Public Release (http://www.dtic.mil/defenselink/dd5230_9.html)

c. DoDI 5120.4, 29 May 96, subject: Electronic Newspaper Policy. (http://www.dtic.mil/defenselink/5120_4.html)

d. DoDI 5230.29, 6 May 96, subject: Security Policy Review of DoD Information for Public Release. (http://www.dtic.mil/defenselink/5230_29.html)

1-3. Department of The Army.

Guidance 30 Oct. 96, HQ DA Washington DC, Guidance for the Management of Army Websites. (http://www.army.mil/da_web_guidance.htm)

1-4. Department of the Air Force (http://www.af.mil/webpolicy/).

a. Air Force Instruction 33-129, 1 January 97, Transmission of Information Via the Internet. The above reference provides a link to download a .pdf type file of this instruction.

b. Air Force Instruction 35-205, 25 February 94, Air Force Security and Policy Review Program. The above reference provides a link to download an executable (.exe) .zip type file of this instruction.

c. Secretary of the Air Force Memorandum, 25 May 96, subject: Clearance Procedures for Making Electronic Information Available to the Public. (http://www.af.mil/webpolicy/policy.htm)

d. CSAF Memorandum, undated, subject: Interim Internet Guidance (http://www.af.mil/webpolicy/interim.htm)

e. HQ USAF Memorandum, 11 March 97, subject: Air Force Electronic Bulletin Boards and Internet World Wide Web Home Pages (http://www.af.mil/webpolicy/auditmsg.htm)

1-5. Department of The Navy.

Chief of Naval Operations, Naval Message ALCOM 035/95, 21 July 95, subject: Guidelines for Naval Use of the Internet // SSIC: N02250 (http://www.chinfo.navy.mil/navpalib/Internet/navyinet.txt)

1-6. National Guard Bureau.

a. All States Letter P96-0052, 5 Apr. 96, subject: Policy on the Use of the Internet.

b. All States Letter P95-0088, DARNG, NGB-AIS, 1 Jun. 95, subject: Use of Electronic Mail (E-mail).

c. Air National Guard Instruction 33-101, Communications, Internet and Electronic Mail Policy.

Section 2
Related Publications

A related publication is merely a source of additional information. The user does not have to read it to understand this regulation.

2-1. US Public Law.

a. Public Law 100-235, Computer Security Act of 1987.

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

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

2-2. New York State Policies (http://www.irm.state.ny.us).

Governor's Task Force on Information Resource Management, Technology Policy 96-11, Subject: NYS Network Services Agenda, 7 August 96.

2-3. Department of Defense (http://www.dtic.mil/defenselink/about.html).

a. Deputy Sec of Defense Memorandum 2 September 95, subject, Government Information Locator Service (GILS). (http://www.dtic.mil/c3i/gilsplcy.html) with attachment (http://www.dtic.mil/c3i/gilsatt.html).

b. Chairman of the Joint Chiefs of Staff Instruction, CJCSI 6211.02, Enclosure A, 23 June 93, subject: Defense Information System Network and Connected Systems.

c. Guidelines, Office of the Assistant Secretary of Defense (Public Affairs), 28 Dec 95, Guidelines for Establishing and Maintaining a Department of Defense Web Information Service (http://www.dtic.mil/defenselink/webguide.html).

d. Defense Information Systems Agency. Mission, Organizational Structure and Internet Information and policy (http://www.disa.mil/disc/discww3.html).

2-4. Department of The Army.

a. AR 25-1, The Army Information Resource Management Program.

b. AR 25-5, Information Management for the Sustaining Base.

c. AR 25-55, Army Freedom of Information Act Program.

d. AR 25-400-2, The Modern Army Recordkeeping System (MARKS).

e. AR 340-21, Army Privacy Act Program.

f. AR 360-6, Public Information.

g. AR 380-5, DOA Information Security Program.

g. AR 380-19, Information System Security.

h. DA Pam 25-1, Army Information Architecture.

I. DA Pam 25-1-1, Installation Information Services.

2-5. Department of The Air Force.

a. AFPD 37-1, Air Force Information Management.

b. AFPD 35-2, Public Communications Programs.

c. AFPD 33-1, Command, Control, Communications, and Computer (C4) Systems.

d. AFPD 33-2, C4 Systems Security.

e. AFPD 31-4, Information Security.

f. AFI 37-131, Air Force Freedom of Information Act Program.

g. AFI 37-132, Air Force Privacy Act Program.

h. AFI 37-138, Records Disposition -- Procedures and Responsibilities.

I. AFMAN 37-123, Management of Records.

j. AFMAN 37-124, Preparing Official Communications, and Interim Guidance on Electronic mail.

k. AFMAN 37-139.

2-6. Department of The Navy.

a. SECNAVINST 5720.44A, U.S.Navy Public Affairs Regulations.

b. SECNAVINST 5211.5D, Department of the Navy Privacy Act Program.

c. OPNAVINST 5510.1H, Department of the Navy Information and Personnel Security Program Regulation.

d. OPNAVINST 2710, Navy Local Area Networks Policies.

e. OPNAVINST 5239.1A, ADP Security Policy.

2-7. Defense Information Systems Agency (DISA).

DISA Instruction 630-225-7, Information Services, Internet, Intranet, and World Wide Web. (http://www.disa.mil/info/disawwwg.html).

2-8. Division of Military & Naval Affairs

DMNA Reg 25-1, Communications and Information Management Program.

THIS

PAGE

INTENTIONALLY

LEFT

BLANK

Appendix B, Glossary

Section I Abbreviations & Acronyms

AFCA
Air Force Communications Agency

AFI
Air Force Instruction

AFIWC
Air Force Information Warfare Center

AFMAN
Air Force Manual

AFPD
Air Force Policy Directive

AFRES
Air Force Reserve

AFSSI
Air Force Systems Security Instruction

AFSSM
Air Force Systems Security Memorandum

AIF/.aiff
a sound file format

APOC
Automation Point of Contact

AR
Army Regulation

ARNG
Army National Guard

AU/.au
a sound file format

BPS
Bits per Second

CERN
The European Laboratory for Particle Physics. The originators of the HTTP and HTML concepts

DA
Department of the Army

DA Cir
Department of the Army Circular

DA Pam
Department of the Army Pamphlet

DDN
Defense Data Network

DISA
Defense Information Systems Agency
www.disa.mil

DMNA
Division of Military and Naval Affairs

DNS
Domain Name System

DOD (DoD)
Department of Defense

DODD (DoDD)
Dept of Defense Directive

DON
Department of the Navy
www.navy.mil

DSN
Defense Switched Network

DTIC
Defense Technical Information Center
www.dtic.mil

E-MAIL (Email)
Electronic Mail

FAQ
Frequently Asked Questions

FM
Field Manual

FOA
Field Operating Agency

FOIA
Freedom of Information Act

FTP
File Transfer Protocol

GIF/.gif
Graphical Interchange Format, an image file format. Compuserve standard for the Internet

GILS
Government Information Locator Service

HQ
Headquarters

HTML
HyperText Markup Language

HTTP
HyperText Transport Protocol, the protocol used by the WWW servers.

IP
Internet Protocol

ISO
The International Organization for Standardization

ISP
Internet Service Provider

JPG / JPEG
Joint Photographic Expert Group, a method of storing an image in digital format.

LAN
Local Area Net

MACOM
Major Command (Army Acronym)

MAJCOM
Major Command (Air Force Acronym)

MIME
Multiple Internet Mail Extensions

ML
Military Law, State of New York

MPEG
Moving Pictures Expert Group, a method of storing moving files in digital format.

NCSA
The National Center for Supercomputing Applications. NCSA is located at the University of Illinois.

NGB
National Guard Bureau

NGR
National Guard (Bureau) Regulation.

NIPRNET
Non-Secure Internet Protocol Router Network

NNTP
Network News Transfer Protocol

NYANG
New York Air National Guard

NYARNG
New York Army National Guard

NYG
New York Guard, a nonfederal state militia force

NYNM
New York Naval Militia, a non-federal state naval militia force. Utilizes dual membership of USNR and USMCR members.

OPNAVINST
Chief of Naval Operations Instructions

OPR
Office of Primary Responsibility

OPSEC
Operations Security

POC
Point of Contact

PPP
Point-to-Point Protocol

RFC
Request for Comments, there are agreed upon standards with which all methods of communicating over the Internet are defined.

SECNAVINST
Secretary of the Navy Instructions

SEMO
State Emergency Management Office

SGML
Standard Generalized Markup Language, is an international standard, an encoding scheme for creating textual information. HTML is a subset of SGML.

SLIP
Serial Line IP

SMTP
Simple Mail Transfer Protocol

SSL
Secure Sockets Layer

TAG
The Adjutant General

TB
Technical Bulletin

TC
Training Circular

TCP/IP
Transmission Control Protocol/ Internet Protocol, a set of rules that establish the method with which data is transmitted over the Internet between two computers.

TIFF/.tif
Tag Image File Format, a file format used for storing image files.

TM
Technical Manual

UCMJ
Uniform Code of Military Justice

URL
Uniform Resource Locator

USAF
United States Air Force
www.af.mil

USN
United States Navy
www.navy.mil

WAIS
Wide Area Information Server, a database.

WAN
Wide Area Net

WWW
W3
World Wide Web, The Web

XBM
X bit map, a simple page format. XBMs only appear in black and white and you will find them in-line in HTML documents.

Section II
Terms

Application
(a) Software that performs a particular useful function for you. ("Do you have an electronic mail application installed on your computer?", A browser?)
(b) The useful function itself (e.g., transferring files is a useful application of the Internet)

Archie
A method of searching for files on anonymous FTP servers.

Army Regulation
A directive that sets forth missions, responsibilities, and policies and establishes procedures to ensure uniform compliance with those policies, Army wide.

Baud
When transmitting data, the number of times the medium's "state" changes per second. For example: a 2400-baud modem changes the signal it sends on the phone line 2400 times per second. Since each change in state can correspond to multiple bits of data, the actual rate of transfer may exceed the baud rate. See also bits per second.

Bits per Second (bps)
The speed at which bits are transmitted over a communications medium.

Browser
It is the World Wide Web client tool used to retrive information from the WWW. Some used are Air Mosaic, Mosaic, Netscape, MS Explorer, and Net Cruiser.

Circular
A publication of agencywide or commandwide application that contains information of general interest and instructions that are temporary or of a one-time nature.

Client
A software application that works on your behalf to extract a service from a server somewhere on the network. NCSA Mosaic is an example of client software.

DA Circular
A temporary directive or informational publication that expires 2 years or less after date of issue.

DA Pamphlet
A permanent instructional or informational publication. The two basic types of pamphlets are standard and informational. A standard pamphlet is organized and printed in the same format as an AR. An informational pamphlet has no set organization or format

Defense Data Network
A portion of the Internet which connects to U.S. military bases and contractors; used for non-secure communications. MILNET is one of the DDN networks. It also runs the NIC where a lot of Internet information is archived.

DefenseLINK
The Official World Wide Web Information Service from the DoD, and the starting point for locating information on Defense servers around the world. www.dtic.mil/defenselink/

DMNA Pamphlet
A permanent instructional or informational publication. The two basic types of pamphlets are standard and informational. A standard pamphlet is organized and printed in the same format as an AR. An informational pamphlet has no set organization or format. Applies to DMNA.

DMNA Regulation
A directive that sets forth missions, responsibilities, and policies and establishes procedures to ensure uniform compliance with those policies, DMNAwide.

Domain Name System
A distributed database system for translating computer names (or URLs like dmna.state.ny.us) into numeric Internet addresses (like 167.152.147.39), and vice versa. DNS allows you to use the Internet without remembering long lists of numbers.

External Viewer
A program used by Browser when Browser cannot handle a particular file internally. For example .ps or postscript files. When the Browser retrieves a .ps file it will pass the file to a postscript viewer and that viewer will display the file to the user.

Field Manual
A DA publication that describes Army doctrine and tactics for implementation. Fms also implement ratified international standardization agreements and are normally the basis for development of training materials.

File Transfer Protocol (FTP)
A protocol for file transfer between computers; transferring files efficiently and reliably among computers and allowing the convenient use of remote file storage capabilities. A transfer protocol used to transfer files from one computer to another

Firewall
A protection scheme that assists in securing internal systems from external systems.

Flame
A virulent and (often) largely personal attack against the author of a USENET posting. Flames are unfortunately common. People who frequently write flames are known as "flamers" (jerks and unproffesional also come to mind)

Gateway
A computer system that transfers data between normally incompatible applications or networks. It reformats the data so that it is acceptable for the new network (or application) before passing it on. A gateway may connect two dissimilar networks, like DECnet and the Internet, or it might allow two incompatible applications to communicate over the same network (like mail systems with different message formats). The term is often used interchangeably with router, but this usage is incorrect.

Gopher
An information transfer protocol based on a menu interface. Gopher is a distributed document search and retrieval system; it combines the best features of browsing through collections of information and fully indexed databases. The protocol and software follow a client-server model, and permits users on a heterogeneous mix of desktop systems to browse, search, and retrieve documents residing on multiple distributed server machines.

Home Page
A top level document of an organization or a document that a user frequently visits. By default you can set your browser to go to a starting Home Page.

Hotlist
A user defined list of preferred URLs to a given World Wide Web Document.

Hyperlink
A link in a given document to information within another document. These links are usually represented by highlighted words or images. The user also has the option to underline these hyperlinks

Hypermedia
Richly formated documents containing a variety of information types, such as textual, image, movie, and audio. These information types are easily found through hyperlinks.

Hypertext
A method for storing, retrieving, and presenting information based on the processing power of computers. Allows computerized linking and almost instantaneous retrieval of information based on a dynamic index.

HyperText Markup Language (HTML)
The rules that govern the way we create documents so that they can be read by a WWW Browser. Most documents that are displayed are HTML documents. These documents are characterized by the .html or .htm file extension.

Hypertext Transfer Protocol (HTTP)
It is the primary protocol used to communicate on the WWW.

Infostructure
A group of web documents linked together on one or more servers, usually providing information concerning a certain subject or idea.

Information Provider
The person or organization that provides information for posting on the Internet.

In-Line image
A graphic that is displayed with an HTML document.

Internet
(a) Generally (not capitalized), any collection of distinct networks working together as one.
(b) Specifically (capitalized), the World-Wide "network of networks" that are connected to each other, using the IP protocol and other similar protocols. The Internet provides file transfer (FTP), rmote login, electronic mail, news, and other services. The combined name for the providers of registration, information, and database services to the Internet. It provides many network resources of its own.

Internet Protocol (IP)
The most important of the protocols on which the Internet is based. It allows a packet to traverse multiple networks on the way to its final destination.

Internet Protocol (IP) Spoofing
The use of software to change the address of a data packet to make it appear to come from another machine. Many network routers use these IP addresses to identify which machines have valid access rights to the network. Spoofing allows a hacker to "change his identity" and appear as a valid machine within the network. This type of attack can be foiled by the filtering router which drops "outside" packets with an "inside" source address.

Internet Service Provider
A commercial entity providing data connectivity into the Internet.

Intranet
A restricted-access network that works like the Web, but isn't on it. Usually owned and managed by an organization, an Intranet enables a activity to share its resources with its employees without sensitive information being made available to everyone with Internet access. Intranets may allow connection outside of the Intranet to the Internet through firewall servers and other security devices that have the ability to screen messages in both directions so that the organizations security is maintained.

Limited Access
Limited access of Internet information applies to information that has been approved for limited access. This information has added safeguards that limit the access to a specific group or groups. The OPR must determine the appropriate security and access controls required to safeguard the information.

Limited Access by Domain
Limiting access by using the domain name (for example, .mil, .gov, .edu, and so forth) to restrict access of an area to a specific group or subgroup. Domains are established by the Internet Engineering Task Force (IETF) and assigned based on function or geography.

Limited Pages
Web pages intended for viewing by a limited audience.

Military Controlled Access Paths
Nonclassified networks or "links" that are leased, configured, managed, and secured by a government agency. This includes the unclassified but sensitive Internet Protocol Router Network (NIPRNET-AF, previously AFIN [Air Force Internet]) as well as dedicated links that have a node on the base network.

MILNET
One of the DDN networks that make up the Internet; devoted to non-classified military (U.S.) communications.

Multiple Internet Mail Extensions (MIME)
A method of identifying files such that the first packet of information received by a client, contains information about the type of file the server has sent. For example, text, audio, movie, postscript, word document, etc...

Network News Transfer Protocol (NNTP)
Also known as Usenet, specifies a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream-based transmission of news among the Internet community. NNTP is designed so that news articles are stored in a central database, allowing a subscriber to select only those items he wishes to read. Indexing, cross-referencing, and expiration of aged messages are also provided.

NGB Pamphlet
A permanent instructional or informational publication. The two basic types of pamphlets are standard and informational. A standard pamphlet is organized and printed in the same format as an AR. An informational pamphlet has no set organization or format. Applies to the National Guard.

National Guard Bureau Regulation
A directive that sets forth missions, responsibilities, and policies and establishes procedures to ensure

uniform compliance with those policies, National Guard wide.

NYARNG Pamphlet
A permanent instructional or informational publication. The two basic types of pamphlets are standard and informational. A standard pamphlet is organized and printed in the same format as an AR. An informational pamphlet has no set organization or format. Applies to the NYARNG.

NYARNG Regulation
A directive that sets forth missions, responsibilities, and policies and establishes procedures to ensure uniform compliance with those policies, NYARNG wide.

Page Maintainer
The creator and, or focal point for specific material posted on the organization's home page.

PostScript
A page description language developed by Adobe Systems.

Proponent
The agency or command responsible for writing and issuing a publication.

Protocol
A planned method of exchanging data over the Internet.

Proxy Server
A server connected to the Internet through which all incoming and outgoing requests go through; used to enhance security and increase performance/efficiency.

Public Access
Public access of Internet information applies to information approved for unlimited public release. Public access information has no access or security controls to limit access to the information. This review determines degree of releasability only; actual release of the material is the decision of the originator (OPR).

Public Pages
Web pages intended for viewing by the general public. Information on these pages should be of interest to the general public.

Publications
The establishment of publications policies, standards, systems, and techniques and there effective and economical use. Publications management extends from the creation of information through the end use of that printed information.

QuickTime
A method of storing movie and audio files in digital format. Developed by Apple Computer.

Secure Sockets Layer (SSL)
A security protocol that provides privacy over the Internet. The protocol allows client/server applications to communicate, while preventing eavesdropping. Servers are always authenticated and clients are optionally authenticated. Server—Software residing on an appropriate hardware platform (computer) that provides a service to other computers or programs, by satisfying client requests.

Serial Line IP
A protocol that allows a computer to use the Internet protocols (and become a full-fledged Internet member) with a standard telephone line and a high-speed modem. SLIP is being superseded by PPP but is still in common use.

Server
(a) Software that allows a computer to offer a service to another computer. Other computers contact the server program by means of matching client software.
(b) The computer on which the server software runs.

Service Provider
An organization that provides connections to a part of the Internet. If you want to connect to your company's network, or even your own PC, to the Internet, you have to talk to a service provider.

Signature
A file, typically five lines long or so, that people often insert at the end of electronic mail messages or USENET articles. A signature contains, minimally, a name and E-mail address.

Simple Mail Transfer Protocol (SMTP)
The protocol used to send electronic mail on the Internet.

Technical Bulletin
A publication that contains information, procedures, and techniques of a technical or professional nature relating to equipment and general subjects.

Technical Manual
A publication that is one of the two types below.
a. Equipment Technical Manual.
b. General subject technical manual.

TELNET
Also known as rlogin, TELNET starts a remote session by specifying a computer to connect to. The command and program used to log in from one Internet site to another. The TELNET command/program gets you to the "login:" prompt of another computer or computer system. From that time until you finish the session, anything you type is sent to the other computer. computer system using the TELNET protocol.

Timeout
A "timeout" is what happens when two computers are "talking" and one computer - for any reason - fails to respond. The other computer keeps on trying for a certain amount of time, but eventually "gives-up" and displays a "timed-out" message.

Training Circular
A permanent DA publication that describes the techniques, procedures, references, or instructions that provide the details of how to implement the

fundamental principles of Army doctrine. They also implement ratified international standardization agreements.

Transmission Control Protocol/Internet Protocol (TCP/IP)
The most accurate name for the set of protocols known as the "Internet Protocol Suite." TCP and IP are two of the protocols in this suite. Because TCP and IP are the best known of the protocols, it has become common to use the term TCP/IP or IP/TCP to refer to the whole family. TCP (the "transmission control protocol") is responsible for breaking up the message into datagrams, reassembling them at the other end, resending anything that gets lost, and putting things back in the right order. IP (the "Internet Protocol") is responsible for routing individual datagrams.

Trojan Horse
A malicious program designed to break security or damage a system that is disguised as something else benign, such as a directory list, archive, a game, or a program to find and destroy viruses.

Uniform Resource Locator
The standardized way in which any resource is identified within a web document or to a web browser. Most URLs consist of the service, host name, and directory path. An example of a URL:
http://www.dmna.state.ny.us
This can be extended with directory path and page: e.g. ***/dmna/jobs.html***

UNIX
A popular operating system (like MS-DOS) that was (and is) very important in the development of the Internet. A majority of Internet servers are UNIX systems.

Web Browser
Software that acts as a client, allowing a person to retrieve information from various sources on the WWW.

Web Document
A physical or logical piece of information on the WWW.

Web Page
Asingle document that includes the text of the document, its structure, any links to other documents, images, and other media. Web Server—A software/hardware combination that provides information resources to the WWW.

Web Server Administrator
The system administration for the web server, usually referred to as the "Webmaster."

Word processing
The equipment and functions associated with the automatic preparation of documents. Included are dictating and transcribing of text and the keyboarding, recording, editing, and revising of text on magnetic media for final output on either modified typewritters or high-speed printers. Word processing equipment is considered composition equipment when the majority of materials prepared are camera-ready copy intended for printing.

World Wide Web (WWW)
Uses the Internet as its transport media and is a collection of protocols and standards that allow the user to find information available on the Internet by using hypertext and/or hypermedia documents.

Suggested Improvements. The proponent office of this regulation is the Directorate of Communications and Information Management (MNCM). Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to The Adjutant General, Division of Military and Naval Affairs, ATTN: MNCM-AS, 330 Old Niskayuna Road, Latham, NY 12110-2224.

OFFICIAL:

JOHN H. FENIMORE, V
Major General, NYANG
The Adjutant General

for DANIEL J. TRAVERS
LTC, SC, NYARNG
Assistant Adjutant General

DISTRIBUTION:
AA
BB, BR
C
D
E
F1-F8
G
S
A - D SEMO