

7 July 2000

Information Management: Automation

**NETWORK SERVICES**

**Summary.** TRADOC's mission and decentralized organization necessitate the use of network services. This regulation establishes command-wide policy for managing, operating, and using network services, specifically electronic mail (E-mail) and Internet services, to include the World Wide Web (WWW).

**Applicability.** This regulation applies to all TRADOC managers, operators, and users of TRADOC-provided network services.

**Supplementation.** Supplementation is authorized as required to amplify local policy for the management, operation, and use of network services. Forward one copy of supplement to Commander, TRADOC, ATTN: ATIM-I, 90 Ingalls Road, Fort Monroe, VA 23651-1065, within 10 days of publishing.

**Suggested improvements.** The proponent of this regulation is the Deputy Chief of Staff for Information Management (DCSIM). Send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) through channels to Commander, TRADOC, ATTN: ATIM-I, 90 Ingalls Road, Fort Monroe, VA 23651-1065. Suggested improvements may also be submitted using DA Form 1045 (Army Ideas for Excellence Program (AIEP) Proposal).

**Availability.** This publication is available on the TRADOC Homepage at <http://www.tradoc.army.mil/tpubs/regndx.htm>.

**Summary of Changes.** This revision-

- \* Changes the Terminal Area Security Officer (TASO) to Information System Security Officer (ISSO) IAW AR 380-19.
- \* Adds clarification of automated data processing position qualifications and background investigation requirements.
- \* Adds clarification of guidelines for network access and services for personnel in the Personnel Exchange Program, Foreign Liaison Office and foreign students.
- \* Adds requirement for programs servicing non-military individuals to arrange for commercial Internet service provider connections.
- \* Adds requirement for users to report incidents with potential or demonstrated impact to the network IAW AR 380-19.
- \* Adds requirement for installations to use a two-tiered virus checking architecture.
- \* Adds guidance for connection of on-post quarters to the CAN.
- \* Adds restriction on use of third-party E-mail services for official business.
- \* Changes E-mail address naming conventions.
- \* Adds restrictions on the use of commercial Internet service providers.
- \* Changes homepage warning banner requirement.
- \* Adds requirement to use a disclaimer statement on web pages with links to external sites.

**Contents**

	Paragraph	Page		Paragraph	Page
Purpose .....	1	2	Internet .....	7	8
References .....	2	2	World Wide Web .....	8	9
Explanation of abbreviations .....	3	2			
Responsibilities .....	4	2	<b>Appendix A</b>		
General policies .....	5	4	References .....		10
E-mail .....	6	6	Glossary .....		10

\* This regulation supersedes TRADOC Regulation 25-70, 1 July 1997.

**1. Purpose.** This regulation prescribes policy and assigns responsibilities within TRADOC for managing, operating, and using common user network services. Common user network services, e.g., E-mail, WWW, and Internet access, support a wide spectrum of TRADOC's business processes. They do not include services specific to a functional area application. Command-wide policies for using and operating common user network services will enhance TRADOC's efficiency and effectiveness in exchanging information and coordinating actions. TRADOC's objective is the maximum availability of network services, at an acceptable level of risk, for the execution of official business.

**2. References.** Appendix A contains required publications.

**3. Explanation of abbreviations.** Abbreviations used in this regulation are explained in the glossary.

**4. Responsibilities.**

a. DCSIM will—

(1) Define policies, procedures, and technical standards, as required, to ensure command-wide interoperability of network services.

(2) Prescribe preferred products lists and product-specific implementation procedures, as required, for command-wide interoperability.

(3) Prescribe measures to control access, input, and use of network services.

(4) Review and process waiver requests for acquisition of E-mail products that are not compliant with Defense Message System (DMS).

(5) Serve as TRADOC Webmaster, to include promulgating policies, procedures, and technical standards for the development, presentation, and maintenance of TRADOC websites. Manage the information content of the top level TRADOC homepages.

b. Installation commanders will—

(1) Oversee the planning, management, operation, and use of installation level network services at their assigned installation and facilities. Ensure the availability of common user network services to users with valid requirements.

(2) Manage installation level communications networks and operate assigned network components, e.g., routers and switches, essential to provision of network services. Ensure components that are jointly controlled by the Directorate of Information Management (DOIM) and another agency (e.g., Army Signal Command) are managed to provide effective security and necessary network services. Ensure installation level communications network capabilities support required network services.

(3) Manage the installation-wide computer architecture that supports network services. Oversee the distribution of networked computer servers or hosts.

(4) Oversee the acquisition of E-mail software packages for use on their installation. Ensure interoperability among the installation's users and interoperable interfaces with other TRADOC installations. Ensure local interoperability with DMS.

(5) Oversee the appointment of system administrators (SAs) and network managers (NMs) who fulfill responsibilities described below for assigned servers and services. Establish standard operating procedures for SAs, as necessary, to ensure installation-wide interoperability and security of network services.

(6) Ensure SAs, NMs, Information System Security Managers (ISSMs) and Information System Security Officers (ISSOs) are certified as required by the Army Information System Security (ISS) program.

(7) Oversee Internet connectivity for installation servers and hosts.

(a) Manage the assignment of Internet Protocol (IP) addresses to servers and hosts. Enforce the use of Army and Internet conventions for server and host addresses.

(b) Implement Army procedures for managing any subdomain(s) established at the installation. Appoint a subdomain administrator for each subdomain, who will be responsible for its overall management, and a subdomain technical point of contact, who will be responsible for its daily operations.

(c) Ensure host and server addresses are properly registered with the Domain Name System (DNS).

(8) Enforce ISS as applicable to the installation's network services.

(a) Implement ISS system architecture mandates, system protection features and procedural security measures to minimize the potential for fraud, misappropriation, unauthorized disclosure, loss of data, or misuse.

(b) Ensure accreditation of assigned networks, stand-alone computers, peripherals and devices are accomplished IAW AR 380-19.

(c) Review and approve requests from contractors and foreign military members for installation network access. Ensure Freedom of Information Act (FOIA) (AR 25-55), Privacy Act (AR 340-21), and Security (ARs 380-19 and 380-67) requirements are met.

(9) Appoint an installation webmaster to oversee the operations and content management of all installation websites. Approve the establishment of all publicly accessible websites operated on hosts on their installation.

c. In direct support of HQ TRADOC, the Commander, Fort Monroe will—

(1) Appoint the SA for the servers hosting the TRADOC website to control file space and provide maintenance and backup of files.

(2) Establish procedures, in coordination with DCSIM, for assignment of web space to unique information providers and for uploading information to the TRADOC web server.

d. For their assigned systems, system administrators and network managers will—

(1) Operate the hardware and software applications, as necessary, to provide required network services. Implement the standard procedures defined by higher headquarters to optimize interoperability and ISS across the DoD.

(2) Execute backup and recovery procedures for the users' data.

(3) Assign USERIDs to users authorized to access their networked system. Verify users' security clearances and background checks (see para 5a(3)) are consistent with the requirements for accessing their system. Delete inactive USERIDs from their system. In coordination with their system's ISSOs, ensure users' training is maintained in accordance with (IAW) the Army ISS program.

(4) Resolve user problems with network services hosted on assigned systems.

(5) Keep users informed of network status.

(6) Identify and coordinate all communications network requirements with the DOIM.

(7) Maintain password security IAW AR 380-19.

(8) Notify the supporting DOIM about failure of networking components.

(9) Prepare and submit registration and registration changes for users, in coordination with the subdomain administrator, through the Army Domain Manager (ADM) to the DoD Network Information Center (NIC).

e. Subdomain administrators will—

(1) Operate their subdomain IAW HQDA, ADM, and Internet technical standards and practices, specifically including the DNS.

(2) Prepare and submit registration and registration changes of subdomain assets (e.g., servers and gateways), through ADM, to the DoD NIC.

(3) Coordinate with the ADM changes and deletions for the subdomain's addresses.

f. Installation ISSMs, IAW AR 380-19, will—

(1) Define installation level security policies and procedures to ensure installation-wide integrity of network services.

(2) Ensure SAs conform to procedures for accreditation of networked components.

(3) Ensure ISSOs are appointed on orders and for each separate automated information system (AIS), group of AIS, or network, as necessary, and understand their responsibilities.

(4) Coordinate security training relevant to network services at their installation.

(5) Advise the installation DOIM on National Security Agency certified information security and network security products.

g. Information System Security Officers will—

(1) Implement security procedures for the network services provided by their assigned systems.

(2) Ensure operators and users for their assigned systems understand their security responsibilities for network services.

(3) Report information security incidents regarding network services to the ISSM.

(4) Ensure all software downloaded using networking services from any source is virus free prior to loading on their assigned systems.

(5) Execute duties stated in AR 380-19 for assigned servers and workstations with access to network services.

(6) Ensure users meet security and disclosure requirements. Notify the ISSM immediately, in writing, of a security clearance or background check that is returned as disapproved.

h. Designated records managers, records coordinators, and records custodians will monitor the application of records management procedures IAW AR 25-400-2 to electronic records.

i. Installation webmasters will—

(1) Provide technical assistance to developers of WWW pages.

(2) Maintain registration of all publicly accessible websites with both HQ TRADOC and the Army website. Registration can be done at <http://www.tradoc.army.mil/webreg/>.

(3) Establish local procedures for review and clearance of information posted to the installation websites.

(4) Ensure installation websites comply with current DoD and Army policy which, can be found at <http://www.army.mil/webmasters/>. Establish local policy as required.

(5) Maintain information integrity of installation websites by using analysis tools to resolve user access errors.

(6) Provide information about local operations as requested by the TRADOC webmaster.

j. Public Affairs Officers (PAO), ISSMs, and Staff Judge Advocates (SJA), at headquarters and installation level, will review materials, as requested by commands, units, or organizations, prior to posting on a publicly accessible WWW or file transfer protocol (FTP) server.

k. TRADOC users of network services will—

(1) Use government-provided access to network services for official business and authorized purposes only (see para 5b).

(2) Ensure they do not process, post, or transmit classified information via unclassified networks. Ensure Army information made available to the general public on the Internet, via the WWW or FTP, is cleared with the functional proponent for public dissemination.

(3) Apply information security guidance in the transmission or posting of data that is unclassified, but covered by the Privacy Act of 1974, sensitive government information, pre-award contractual information, resource accounting data, trade secrets or non-government information being retained on a confidential basis.

(4) Notify ISSO of possible security compromises, virus contamination through file transfer/execution or E-mail, and forgotten passwords.

(5) Safeguard their passwords from use by other users unless granted an exception to policy by the ISSM.

(6) Observe procedures defined by their ISSO for ensuring software downloaded using network services is virus free prior to loading on a TRADOC system.

**5. General policies.** This paragraph provides policies regarding authorized access and uses of TRADOC-provided network services.

a. Per assigned responsibilities in paragraph 4, TRADOC organizations will control access to network services.

(1) SAs will establish accounts and assign USERIDs for individuals with a need for network services. SAs will revoke USERIDs that have been inactive for 90 days or more, unless an exception has been granted. ISSOs will request any required exceptions from the supporting ISSM.

(2) Users with network access to classified information will possess a valid security clearance appropriate to their level of access. Users will in-process and out-process with their ISSO or SA as a control on the addition and deletion of accounts for network services.

(3) Army personnel security policies coupled with "least privileged access" apply to the determination of whether an individual is authorized access to network services. Per AR 380-19, determination for a background check is based on the level of automated data processing (ADP) sensitivity and the ADP position requirements. Criteria for occupying ADP I, II, or III positions are contained in AR 380-67, appendix K. An AIS user whose position does not fit the definition of ADP-I or ADP-II is considered to be in an ADP-III position. Investigations for all personnel selected for any ADP position must be completed before the individual is permitted access to an AIS and placed in an ADP position. Exceptions for ADP-I and ADP-II positions are outlined in AR 380-67. In TRADOC, these exceptions also apply to ADP-III positions.

(4) Personnel Exchange Program (PEP) officers may be provided network services. PEP officers are military or civilian officials of foreign governments, assigned to DA activities under Personnel Exchange Program agreements, who perform duties prescribed by a position description for the DA activity.

(a) PEP officers are subject to the same policies and procedures governing use of network services as their U.S. Army coworkers. Additional restrictions on computer system access and access to electronic document repositories are contained in AR 380-10, paragraph 5.30.

(b) Unclassified information which is accessible by the computer system, that is not in the public domain or approved for release to the PEP officer's parent government, must be processed through foreign disclosure channels for adjudication.

(c) PEP officers may only be given access to classified systems if specifically approved through foreign disclosure channels. Classified Military Information (CMI), Privacy Act data, and non-releasable FOIA information will not be released or passed to a PEP officer without prior approval.

(d) Acceptance of a PEP officer's national clearance constitutes meeting the ADP III requirements described in AR 380-19.

(e) Access will be terminated upon expiration of the PEP officer's certification or physical departure from the organization, whichever is earlier.

(5) Foreign Liaison Officers (FLO) may be provided network services. FLOs are foreign government officials, either military or civilian employees, certified by their governments to act as representatives of that government to a DA element. The Delegation of Disclosure Authority Letter is the determining document in deciding what services TRADOC will provide to the FLO. SAs should coordinate with the local Foreign Disclosure Office on a case-by-case basis to determine which services apply to each FLO. Although background investigations IAW 380-19 are not conducted on FLOs, they may be given access to TRADOC unclassified systems for network services, subject to the following procedures and restrictions:

(a) FLOs will use individual USERIDs and passwords for the period they are accredited to the TRADOC organization. The FLO, through the activity responsible for installation FLO support or the local disclosure office, will submit the request for a USERID to the SA for further processing. The Designated Approval Authority for local access to installation managed information systems is the installation commander. Additional restrictions on computer system access and access to electronic document repositories are contained in AR 380-10, paragraph 5.28. System access will be terminated upon expiration of FLO accreditation or departure from the organization, whichever is earlier.

(b) The system will be accredited IAW AR 380-19. Additionally, FLOs will not use systems that access

external networks operated by the DoD or U.S. military services except through a DA approved firewall. The firewall will be operated such that IP filtering and communications protocol permissions are configured to explicitly allow FLOs access to authorized network services only, for example, simple E-mail, HTTP, and FTP. The firewall will be configured to explicitly disallow FLOs access to trivial file transfer protocol. Other technical solutions are permissible if they better fit the local architecture, can still provide these same protections, are endorsed by the installation DOIM and ISSM, and are approved for use by the installation commander.

(c) At no time will a FLO be granted access to a classified system. Access will be limited to unclassified releasable information (see para 5a4(b), above). Classified defense information, controlled unclassified information, Privacy Act data, and non-releasable FOIA information will not be released or passed to FLOs.

(d) FLOs will not have access to, nor shall E-mail users pass, information on any third country activities with the U.S. Government/Army.

(e) FLO governments are expected to provide all of the FLOs hardware and software support. For services above and beyond what is provided by the installation infrastructure, the costs will be borne by the parent government. U.S. Government resources may be used at the discretion of the installation commander.

(f) Local FLO support offices will provide or arrange training for all FLOs prior to their access to E-mail services. FLO support offices will advise all FLOs that under no circumstances will personal software be loaded into or used on any computer that is networked with a TRADOC system.

(6) Foreign students may be provided network services. Although background investigations IAW 380-19 are not conducted on foreign students, they may be provided services subject to the same restrictions described in paragraph 5a(5)(a) through (d) for FLOs. Foreign students shall not be given Terminal Server Access Controller System (TSACS) access unless HQ TRADOC has approved the installation's general procedure and architecture for granting such access. Submit rationale and risk assessment through the ISSM to the TRADOC DCSIM.

(7) Requirements for network services and access to ADP systems for Foreign National Employees are outlined in AR 380-19, paragraph 2-17.

(8) Volunteer workers, e.g., Red Cross and Army Community Service, may be provided network services. The sponsoring organization will request service for the individual from the DOIM and provide functional justification as required locally. The DOIM will forward the request, with recommendation, to the responsible commander in the grade of Colonel or above for approval. The following restrictions apply—

(a) The volunteer must be a U.S. citizen.

(b) Individual USERIDs and passwords must be assigned to each volunteer for the period they are volunteers and require service. System access will be terminated upon departure from the organization.

(c) Access will be granted only for unclassified E-mail and publicly releasable information. Volunteers will not be granted access to classified systems.

(9) Military contractors may be provided network services. The sponsoring organization will request service for the individual from the DOIM and provide functional justification as required locally. The DOIM is the approval authority. The DOIM must determine such use is the best technical solution to Army requirements, and that the local architecture can support it with acceptable impact on network performance and acceptable technical risk to other networked components. Contractors must have a clearance or background check completed prior to being assigned to an ADP position.

(a) Military contractors may only be given access to information that is needed under the terms of the contract.

(b) Access will be terminated upon expiration of the contract.

(10) Proponents for programs that require network services for dependents, retirees, and other individuals serviced at TRADOC installations (e.g., Morale, Welfare, and Recreation) will arrange for service by a commercial Internet service provider (ISP). Proponents will coordinate with the ISSO to ensure ISS requirements are met by the network solution. (See para 7d.)

b. TRADOC personnel will limit their use of government-provided network services to official business and authorized purposes. This includes use of government-provided services from the home or during off duty hours, and specifically prohibits Internet access for unauthorized personal use. Inappropriate use of TRADOC network services may be a basis for consideration of disciplinary action and/or denial of network services for any user (e.g., soldiers, civilians, volunteers, contractors, exchange personnel, FLOs).

(1) Authorized purposes can include personal communications that are reasonably made from the workplace, to include communications by E-mail and brief Internet searches, provided such use—

(a) Causes no adverse impact on the employee's official duties.

(b) Is of reasonable duration and during personal time (e.g., before or after the workday, break periods or lunch) as much as possible.

(c) Serves legitimate public interest (e.g., enhancing employee proficiency in use of the system, or enhancing professional skills).

(d) Causes no adverse reflection on DoD.

(2) Authorized purposes also include professional development. Such use will not detract from primary duties and mission accomplishment.

(3) Specific examples of these authorized purposes include, but are not limited to: sending E-mail to build office morale by keeping employees informed of office activities (e.g., office parties, or status of sick employees), sending E-mail to families at home while on temporary duty, making a medical appointment, reading a news magazine at a website, browsing for professional information having general relevance to your official duties, searching for job announcements as a result of government downsizing, and subscribing to professional mail list servers. Authorized purposes will not include sending electronic chain letters or "for sale" messages, fundraising for private enterprises, or conducting a private business, such as a tax preparation service.

(4) Personal use means non-government activity that is conducted for purposes other than outside employment. The Joint Ethics Regulation (JER) specifically prohibits using government equipment for outside employment. Personal use also excludes using government office equipment for activities that are illegal, inappropriate, or offensive to fellow employees or the public. Such activities include gambling, hate speech, sexually explicit materials, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation. The creation, downloading, storage, copying, transmission, or retransmission of chain letters, broadcast transmissions or other mass mailings, regardless of the subject matter, is inappropriate use.

(5) Any use that could cause congestion, delay, degradation or disruption of service to any government system or equipment is inappropriate. For example: video, sound or other large files, "push" technology on the Internet and other continuous data streams, and maintaining a connection to an unofficial "chat room" or instant messaging client.

(6) Installation commanders and supervisors may further restrict the scope of authorized purposes as required (e.g., to relieve the burden on the local network system capabilities or costs, or further limit periods of the duty day during which time is spent on E-mail or the Internet in order to increase worker efficiency).

(7) Use of TRADOC communications resources is not anonymous. In accordance with the JER (Sections 2-301.A (3) and (4)), use of network services, the Internet, E-mail or any AIS serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.

(8) SAs will report possible occurrences of unauthorized use to the soldier/employee's immediate commander/supervisor, who will consider appropriate disciplinary or other corrective action.

c. All users, ISSOs, SAs and NMs of network services will report incidents with potential or demonstrated impact on information system security (e.g., denial of service

attacks, receipt of virus transmissions, breach of passwords) IAW AR 380-19. The reporting channel extends from the user, ISSO, SA or NM, through their servicing ISSO, to the ISSM. Incidents reported to the Army Computer Emergency Response Team will also be reported to the TRADOC Information System Security Program Manager (ISSPM). The ISSM or ISSPM will determine what further action is required.

d. To protect against the spread of computer viruses through network services, installations will use a two-tiered virus checking architecture, (e.g., apply McAfee Anti-Virus (AV) on servers and Norton AV on workstations or vice versa). ISSMs, SAs, ISSOs, and users must ensure DoD approved anti-viral software products are used and that each product's most current version is installed on all devices. Users will employ the virus-check procedures at their level as defined by their ISSO.

e. In accordance with AR 25-1, paragraph 6.3.h, network services are authorized, though not mandated, in personal quarters for key personnel whose duties require immediate response or have a direct bearing on the timely execution of critical actions. Use is restricted to the same authorized uses and ISS protections as described throughout this regulation. If such services are provided, the following special requirements will be met:

(1) Only government-owned systems may be directly connected to the CAN.

(2) Only government-owned software may be installed on the system.

(3) The system must be accredited and maintained IAW AR 380-19 and DODI 5200.40.

(4) The end-user operating system must authenticate the user as having a valid user account prior to granting access to the system. Operating systems that can bypass the logon routine by hitting a key or combination of keys do not meet this requirement.

(5) Users must make the equipment in quarters accessible to the SA for hardware and software maintenance and ISS actions.

**6. E-mail.** This paragraph provides command-wide policies specific to managing, operating, and using E-mail services.

a. Commanders and activity heads will establish and enforce local procedures to minimize improper use of E-mail. Improper uses include:

(1) exploiting list servers or similar group broadcast systems for purposes beyond their intended scope to widely distribute unsolicited E-mail;

(2) sending the same E-mail message repeatedly to one or more recipients to interfere with the recipient's use of E-mail;

(3) sending, or broadcasting, E-mail messages of quotations, jokes, etc., to multiple addressees;

(4) sending or broadcasting unsubstantiated virus warnings from sources other than ISSMs.

b. System administrators for E-mail services will, within the technical capabilities of the software, limit the number of possible addressees for all messages to 100 or less. Users will limit distribution of their messages to addressees within the scope of their organization's mission requirements. Users will target selected addressees when sending large messages, particularly those with file attachments, rather than using a broadcast or sending to a general-purpose distribution list. Instead of broadcasting, users will post non-time sensitive information with broad relevance to electronic bulletin boards or E-mail public folders. With the exception of users responsible for disseminating information organization-wide (e.g., personnel officers, command group, SAs), users will not broadcast to distribution lists for the installation, domain, server or TRADOC school. SAs will advise users on proper use when specific instances of indiscriminate distribution are identified. DOIMs may rescind services if abuse continues.

c. Users will not represent individual user E-mail messages as a TRADOC position unless the same level of coordination and approval has been used in its generation as would be used to develop a signed, paper-based TRADOC position.

d. Users will not conduct official business using commercial E-mail providers (e.g., Hotmail, America Online, etc.). If E-mail access is required while away from the office (e.g., while on TDY) and the office account is not accessible over the Internet, users will obtain an account from a service operated by HQDA, i.e., Army Knowledge Online (<http://ako.us.army.mil/>).

e. When sending files as an attachment to E-mail notes, use the standardized file formats given in TRADOC Pam 25-73 to increase the probability that all addressees can read it. This may require saving the file to an earlier application version than is used to create it.

f. To promote interoperable E-mail services, SAs and subdomain managers will observe TRADOC conventions for formatting directories, network resource addresses, and addresses. For DMS solutions, observe formatting conventions defined by HQDA. For non-DMS solutions, observe this regulation and any supplemental procedures defined in TRADOC-produced reference guides for product specific E-mail solutions. Complete E-mail addresses will follow the format: `username@hostname.domain2`. Since most TRADOC installations and activities belong to the Army domain managed by the ADM, the "domain2" portion of the address will typically read ".army.mil." For servers connected to the secure DoD wide area network (Secret Internet Protocol Routing Network)(SIPRNET), the domain will read ".army.smil.mil."

(1) For individual addresses, the username portion will use the format: `lastname+firstinitial+middleinitial`. For example, James B. Burton would be assigned the username "burtonjb." If necessary, truncate the last name portion to fit within the technical limitations of the particular software being used. If the individual has no middle

name, then leave out that portion. If necessary, use numbers at the end of the string to resolve duplicate names, e.g., "smithja" and "smithja2." Use these formats for all new users. Conversion of previous accounts may be phased through attrition. The subdomain manager may further restrict the format within these parameters.

(2) For the Simple Mail Transfer Protocol (SMTP) alias of the username portion, use the format: `firstname.lastname`, e.g., "james.burton." Use numbers at the end of the string to resolve duplicate names, e.g., "john.smith2." Legacy SMTP aliases may be retained as secondary aliases. Use these formats for all new users. Conversion of previous accounts may be phased through attrition.

(3) Providing contractors, FLOs, PEP personnel, foreign students and volunteers E-mail addresses on servers within the ".army.mil" domain can make E-mail correspondence from them appear to be from an Army employee. To avoid the perception that non-DoD employees using E-mail systems within the Army domain are government officials, SAs will modify the E-mail address alias or directory entries to distinguish their affiliation, e.g., Smith, Bob (Contractor).

(4) For organizational addresses, the username portion will be the same as the office symbol. Aliases are permissible for well known organizational acronyms (e.g., `DCSIM@monroe.army.mil` may be an alias for `ATIM@monroe.army.mil`). Punctuation is permissible (e.g., the username for ATIM-I can be `ATIMI` or `ATIM-I`). The subdomain manager may further restrict the format within these parameters.

(5) See format conventions for the host name portion in paragraph 7c.

g. System administrators will establish an organizational E-mail account for each serviced office (no lower than division level) to receive official correspondence, taskings and messages. Office managers will identify individuals responsible for managing the office's organizational E-mail account and ensure time sensitive messages are acted upon promptly. Minimize the number of users sharing the passwords for office accounts.

h. Electronic mail will be provided 24 hours a day except for scheduled maintenance, periods of severe weather, or emergency maintenance.

i. In accordance with DoD policy, DOIMs and DCSIM will not certify the acquisition of non-DMS compliant E-mail software unless a transition path to full compliance can be documented. Waivers can be granted only at DoD level. Waiver requests will be prepared and submitted to DCSIM for further processing. (Note: DoD defines DMS compliance as electronic messaging and directory support using ITU standard X.400 and X.500 components that have undergone DMS conformance, interoperability and compliance certification by the Joint Interoperability Test Center and are on the certified DMS components list for DoD use.)

**7. Internet.** This paragraph provides command-wide policies specific to managing, operating, and using Internet access.

a. If the installation DOIM determines it is appropriate to establish a local subdomain (a hierarchically related group of Internet addresses) of the higher Army domain, then the DOIM will coordinate its establishment with the ADM. The ADM has specific formats, or templates, for collecting the data necessary to establish a subdomain. The ADM electronically posts procedures on its WWW site. DOIMs must approve all requests for subdomains to be hosted on servers at their installation.

b. The installation DOIM will register and maintain entries for TRADOC operated servers, hosts, gateways, and users in the DoD NIC database. Use procedures posted by the ADM on its WWW site.

c. To promote interoperable Internet services, SAs and subdomain managers will observe the DNS conventions for naming hosts and servers as defined by the ADM. Coordinate names and changes with the ADM.

(1) Installations that do not use a subdomain for structuring a hierarchy of local servers will format servers' or hosts' addresses using the convention: location-server.army.mil. The location will be the first 10 characters of the installation's name (excluding "Fort"), e.g., "eustis-emh1.army.mil." Installations that do use a subdomain for structuring their network will format the servers' or hosts' addresses using the convention: server.subdomain.army.mil, e.g., "emh1.eustis.army.mil." In either case, the server portion of the E-mail address is optional, depending on the local capability to resolve addresses without its use. For example, the alias names for all servers at Fort Eustis may be "eustis.army.mil" if that name can be resolved to individual servers by the network architecture.

(2) If used, the server portion of the E-mail address can take a functional or organizational approach.

(a) In the functional approach, use a code, up to 10 characters, for the server's main purpose. For example, "emh" can be a code for E-mail host and "www" can be a code for a web server. The code can include a sequential number. For example, a host with the address "monroe-emh1.army.mil" would be the first E-mail host at Fort Monroe. There is no mandatory list of codes.

(b) In the organizational approach, use a code, up to 10 characters, that is a well-known name for the organization. For example, "trac.wsmr.army.mil" could be used for a host at the TRADOC Analysis Center at White Sands Missile Range that serves as the E-mail entry and exit point for the whole organization.

d. TRADOC organizations will not use or approve the use of any connections between commercial Internet Service Providers (ISPs) and DoD operated data networks. Instead, TRADOC operated data networks will connect into the Internet through the DoD operated wide area networks. TRADOC and installation organizations are permitted to use commercial ISPs and subscription services (e.g., America On-Line) through computers and

networks that have no network connectivity to TRADOC operated data networks. Such use of commercial ISPs may provide the best technical solution for capabilities required by PEP personnel, FLOs, or dependents. Do not use TRADOC-owned facilities or equipment to access commercial services unless a TRADOC established and managed contract is in place. All TRADOC websites will be hosted on Army or DoD-operated systems. The responsible ISSM must concur with proposals for using commercial ISPs and commercial network services prior to implementation.

e. Ensure electronic material offered or obtained via the Internet is virus free by using virus protection software down to the user level on any computer system(s) accessing or making electronic material available via the Internet.

f. Personnel using the Internet to distribute information through publicly accessible web-sites, bulletin boards, FTP services or similar displays will ensure information they post is cleared by the proponent for the functional content of the information. When requested, PAOs, ISSMs, and SJAs will review materials prior to their posting on a publicly accessible server. Personnel using such Internet services to distribute information will not make accessible the following types of information under any circumstances:

- (1) Classified information.
- (2) Privacy Act information.
- (3) For Official Use Only (FOUO) information.
- (4) Unclassified information that requires special handling, e.g., Encrypt For Transmission Only, Limited Distribution, scientific and technical information protected under the Technology Transfer Laws.
- (5) FOIA exempt information.

g. Coordinate release of any computer program to the public or a contractor, except that which is already public domain, with the SJA. Release of a TRADOC developed program must not compete with any commercially available program.

h. All information posted to a TRADOC managed network service (website, FTP site, etc.) that is publicly accessible through the Internet is considered a Federal record. Unless access to the site can be restricted to appropriate users, TRADOC personnel will not post non-record material such as coordinating draft documents that contain raw data or sensitive information.

i. Use of FTP services, with or without a WWW user interface, is permissible. SAs for servers with network connectivity and FTP capabilities will determine the level of FTP services that can be made available within ISS requirements. SAs will provide technical assistance to organizations with functional requirements for outbound FTP services to ensure both the functional and ISS requirements are optimally met within the capabilities available. To protect against downloading viruses, users will employ the virus-check procedures defined by their ISSO.

j. Prior to user installation of “beta” or pre-release software on any AIS connected to the CAN, the user will obtain written approval from the ISSO and DOIM. This does not apply to installation of software on development AIS.

**8. World Wide Web.** This paragraph provides command-wide policies specific for managing, operating, and using WWW services.

a. As used in this regulation, a homepage is the index or introductory file for a website. It is designed to be the first file accessed by a user visiting a website. A website is a collection of information organized into a number of HTML-compliant files related to a common subject. A website includes a “homepage” and the linked subordinate information. TRADOC activities will determine their local requirements to produce and maintain websites and coordinate their establishment with the installation webmaster. Installation webmasters will register TRADOC installation and major subordinate command homepages with the Army webmaster (webmaster@us.army.mil), the TRADOC webmaster (<http://www.tradoc.army.mil/webreg/>) and the Government Information Locator Service (<http://sites.defenselink.mil/>).

b. Webmasters will maintain familiarity with the website administration policies and procedures defined by DoD and HQDA distributed by memoranda and websites. Webmasters, in coordination with ISSMs, will implement these procedures as applicable to TRADOC managed websites.

c. TRADOC activities that develop websites will observe the command-wide formatting conventions prescribed in TRADOC Pam 25-70, and the following policies:

(1) TRADOC installations and major subordinate commands will include a link from homepages to the Army homepage and to the TRADOC homepage. All other subordinate website pages will include a link to the Army homepage only if registered with the Army site. A link to the Army homepage is mandatory for the HQ TRADOC homepage and the installation homepages. It is not required for the HQ TRADOC staff elements and installation subordinate websites.

(2) Organizational and installation homepages must display a Privacy and Security notice.

(3) Organizational and installation homepages will include (or link to):

(a) A description of the local mission and organizational structure.

(b) Contact information for the webmaster with responsibility for the website content.

(c) An electronic phone directory which lists the commander/chief of the organization and at least one additional layer of the organization by position and phone number (to include major staff elements and sub-organizations). Limit information posted on publicly accessible websites to organizational charts that contain no more information than individuals’ names, duty phone number, duty E-mail address, or office address. If the directory information is on a publicly available web page, then exclude directory entries that may interfere with an organization’s ability to conduct business efficiently, such as direct desktop phone numbers and E-mail accounts for general officers, senior executive service, and Command Sergeants Major (post/installation level and above).

d. Before using information retrieved from the WWW for TRADOC’s official business, ensure such use complies with copyright provisions.

e. Websites can be public or restricted. Public websites use no positive access control; e.g., user authentication or firewalls, to restrict access to information posted on the website. Personnel using websites to disseminate TRADOC information will ensure it is properly cleared (see para 7f). Webmasters will ensure websites within their area of responsibility do not provide methods to bypass access controls (e.g., hyperlinks to web pages below password protected web pages).

f. TRADOC activities have the flexibility to use government or commercial sources for webmaster and authoring support. Select support from the most available, appropriate, and affordable source to adequately perform the mission.

g. TRADOC webmaster will administer a command-wide indexing, or search, capability. Installation webmasters will use a robots.txt file at the root level to indicate which parts of their website should not be visited by indexing robots.

h. Webmasters will monitor the accuracy of links on their websites. At least monthly, webmasters will review error data in their website’s automated access logs and take action to correct link and document access errors.

i. Space provided on websites for use by private organizations must be reviewed and approved by the installation SJA.

j. All links to non-government external WWW resources must include a disclaimer that neither DoD nor the local organization endorses the product or organization at the destination, nor does DoD exercise responsibility over the content at the destination.

**Appendix A**

**References**

DOD 5500.7-R  
Joint Ethics Regulation (JER)

DODI 5200.40  
DOD Information Technology Security Certification and Accreditation Process (DITSCAP)

AR 25-55  
The Department of the Army Freedom of Information Act Program

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

AR 340-21  
The Army Privacy Program

AR 380-10  
Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives

AR 380-19  
Information Systems Security

AR 380-67  
The Department of the Army Personnel Security Program

TRADOC Pam 25-70  
Homepages and Websites

TRADOC Pam 25-72  
Information Systems for TRADOC Organizations and Installations

TRADOC Pam 25-73  
TRADOC Plan for Reengineering Information Systems Modernization (TPRISM)

Army Website Management and Guidance Memorandum ([http://www.army.mil/webmasters/DA\\_Web\\_Guidance.htm](http://www.army.mil/webmasters/DA_Web_Guidance.htm))

**Glossary**

ADM Army Domain Manager

AIS automated information system

CAN campus area network

COR Contracting Officer's Representative

DCSIM Deputy Chief of Staff for Information Management

DMS Defense Message System

DNS domain name system

DOIM Director of Information Management

E-mail electronic mail

FLO foreign liaison officer

FOIA Freedom of Information Act

FOUO For Official Use Only

FTP file transfer protocol

HTML Hypertext Mark-up Language

HTTP hypertext transfer protocol

IAW in accordance with

IP Internet Protocol

ISP Internet service provider

ISS information systems security

ISSM Information Systems Security Manager

ISSO Information System Security Officer

JER Joint Ethics Regulation

NIC Network Information Center

NM network manager

PEP Personnel Exchange Program

RDL General Dennis J. Reimer Training and Doctrine Digital Library

SA system administrator

PAO Public Affairs Officer

PEP Personnel Exchange Program

SJA Staff Judge Advocate

URL uniform resource locator

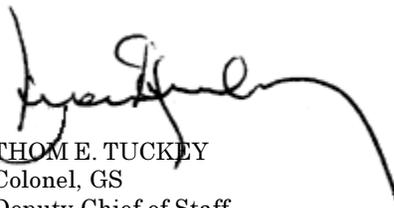
USERID user identification

WWW World Wide Web

FOR THE COMMANDER:

OFFICIAL:

CHARLES W. THOMAS  
Major General, GS  
Chief of Staff



THOM E. TUCKEY  
Colonel, GS  
Deputy Chief of Staff  
for Information Management