UNITED STATES TRANSPORTATION COMMAND
Scott Air Force Base IL 62225-5357

USTRANSCOM INSTRUCTION 33-301
1 March 1997

Communications

COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTER SYSTEMS INTERNET ACCESS AND USE

The Internet is a worldwide network of information resources intended for use as an interactive system for exchanging data. Through the Internet, United States Transportation Command (USTRANSCOM) personnel have immediate access to a wealth of information from academic, scientific, governmental, and commercial databases. However, access to the Internet also presents serious security challenges and significant opportunity for abuse. This document establishes policy on making information available over the Internet, including the World Wide Web (WWW). This instruction addresses information content, access and security controls, presentations, roles and responsibilities, and outlines procedures for properly using, placing, and maintaining information on the Internet. For this instruction, the term Internet includes, but is not limited to, services such as: WWW, Bulletin Board Systems (BBS), File Transfer Protocol (FTP), Telecommunications Networking (TELNET), and Gopher/Browser services. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this instruction does not imply endorsement by USTRANSCOM. Different procedures are established for public access Internet systems and those available to only official users. Violation of this instruction may subject individuals to adverse disciplinary actions under the Uniform Code of Military Justice or the applicable civilian personnel regulations. This instruction is applicable to all personnel (including contractors) assigned or attached to USTRANSCOM, Scott AFB, Illinois, Direct Reporting Units (DRUs), and the Transportation Component Commands (TCCs) , where the subject matter of the Internet material relates to common-user transportation scheduling, or other matters within the purview of the Commander in Chief, USTRANSCOM (USCINCTRANS). This instruction implements USTRANSCOM Policy Directive 33-3, USTRANSCOM Internet Access and Use.

1. References, Abbreviations, Acronyms, and Terms. References, related publications, abbreviations, acronyms and terms used in this instruction are listed in Attachment 1.

OPR: TCJ6-PL (Lt Col Curtis)

Certified by: TCJ6 (Brig Gen Stephen E. Kelley)
Pages 19/Distribution: X (See signature page.)

2. Policy and Procedures:

2.1. Directors/Chiefs, Direct Reporting Elements (DREs), DRUs, and TCCs are expected to maintain adequate controls over Internet access, Internet use and Web page production. They will provide points of contact (POCs) to Command, Control, Communications, and Computer Systems (C4S) Directorate (TCJ6).

2.2. Only software authorized by TCJ6 will be used by USTRANSCOM personnel to access information resources on the Internet. The appropriate Functional Area Communications-Computer Systems Manager (FACCSM) will coordinate with the help desk for authorized software installation on machines for individuals designated in accordance with (IAW) paragraph 2.1.

2.3. All servers that are to be connected to the Internet must have formal, written accreditation from the Designated Approval Authority (DAA), C4S Operations and Security Division (TCJ6-0), or for TCCs, IAW their written procedures, prior to being placed into operation.

2.4. Files created by USTRANSCOM personnel are considered Government records and will always be treated as such. Files will not be transferred to mailing lists or remote hosts, unless it is required in connection with official business.

2.5. No classified, For Official Use Only (FOUO), Freedom of Information Act (FOIA) protected or Privacy Act protected information will be placed on the Internet where the general public can have access to the material.

3. Roles and Responsibilities:

3.1. A command Policy and Implementation Steering Group (P&ISG) will advise the command on public, private, and classified WWW concerns and issues. The working group is chaired by TCJ6 and consists of representatives from Public Affairs (TCPA), Office of Information Management (TCIM), Chief Counsel (TCJA), Inspector General (TCIG), each directorate and the TCCs. The P&ISG will:

3.1.1. Establish and recommend USTRANSCOM development priorities and implementation milestones.

3.1.2. Develop a phased capability program.

3.1.3. Orchestrate working protocol to implement and enforce command WWW policy and procedures.

3.1.4. Support established command business rules applying to public release of USTRANSCOM's transportation business information.

3.1.5. Establish command procedures for submission of information entry onto USTRANSCOM's Web pages.

3.1.6. Provide guidance and recommendations to Directors/Chief, DREs, DRUs, and TCCs to maintain the quality and architectural integrity of USTRANSCOM web pages.

3.2. Command, Control, Communications, and Computer Systems (C4S) Directorate (TCJ6) will:

3.2.1. Manage and administer all servers owned and operated by USTRANSCOM, or located within USTRANSCOM facilities that are maintained for the primary purpose of providing Internet/WWW services. This includes WWW servers, USTRANSCOM "homepage," and the loading of all data on the servers after release has been approved, as applicable. TCCs will keep TCJ6 informed on servers in use with those commands to ensure consistent policies and quality are maintained. (See Attachment 2 for guidelines to establish a web site.)

3.2.2. Establish and orchestrate USTRANSCOM's WWW P&ISG to include designating a chairman from TCJ6.

3.2.3. Update and publish USTRANSCOM policy directives pertaining to Internet access and command procedures.

3.2.4. Create and maintain USTRANSCOM's supporting systems architecture.

3.2.5. Designate USTRANSCOM's Webmaster to serve as a focal point for routine WWW matters.

3.2.6. Establish and enforce security capabilities/protective measures needed to minimize disruption to USTRANSCOM's WWW lines-of-communication.

3.2.7. Utilize "firewall" technology and style guide (USTRANSCOM Handbook 33-302) for page standardization application.

3.2.8. Designate a directorate representative to serve on the P&ISG.

3.2.9. Ensure all internet servers comply with 24 X 7 operations. Appropriate personnel will be identified to address local operational problems and, should outage occur, restore the server as quickly as possible.

3.2.10. TCJ6 Information Systems Security Branch (TCJ6-OS) is responsible for the initial security of the Internet Web pages and the initial investigation of all computer security incidents and any alleged misuse/abuse of Government automated data processing (ADP) assets located at USTRANSCOM. TCCs will conduct initial investigations and coordinate with TCJ6-OS on all incidents involving USTRANSCOM related data/programs on the Internet systems.

3.3. USTRANSCOM Directorates, TCCs, DRUs, and DREs will:

3.3.1. Designate an organizational Point of Contact (POC) to assist USTRANSCOM's Webmaster in the enforcement of security and procedural compliance.

3.3.2. Submit and keep up-to-date information on sponsored web pages IAW established USTRANSCOM policy.

3.3.3. Support and enforce the decisions of the P&ISG.

3.3.4. Conduct initial investigations and coordinate with TCJ6-OS on all incidents involving USTRANSCOM related data/programs on the Internet systems.

3.4. Public Affairs (TCPA) will:

3.4.1. Review and provide recommendations on USTRANSCOM transportation business homepage content. Business homepage includes that material accessible only to .mil, .gov addressees or those with password access to information.

3.4.2. Coordinate with TCIM and TCJA before granting authorization for release of all information on USTRANSCOM's homepages and sub-pages.

3.4.3. Assume and exercise final clearance authority for release of all USTRANSCOM information designated for public access on the WWW.

3.4.4. Support and enforce the decisions of the P&ISG.

3.4.5. Designate a representative to serve on the P&ISG.

3.4.6. Review and coordinate on all public web pages.

3.5. Chief Counsel (TCJA) will:

3.5.1. Conduct and provide legal interpretations pertaining to information release limitations.

3.5.2. Designate a representative to serve on the P&ISG.

3.5.3. Coordinate and review all public Internet page releases and provide legal interpretations.

3.5.4. Support and enforce the decisions of the P&ISG.

3.6. Office of Information Management (TCIM) will:

3.6.1. Coordinate to determine if informational release complies with national Freedom of Information Act (FOIA) and Privacy Act (PA).

3.6.2. Designate a representative to serve on the P&ISG.

3.6.3. Coordinate and review all public Internet page releases.

3.6.4. Support and enforce the decisions of the P&ISG.

3.7. Joint Transportation Corporate Information Management (CIM) Center (JTCC) will:

3.7.1. Create USTRANSCOM's initial operational architecture for conducting Defense Transportation System (DTS) related business transactions via the WWW.

3.7.2. Designate a representative to serve on the P&ISG.

3.7.3. Support and enforce the decisions of the P&ISG.

3.8. Operations and Logistics Directorate (TCJ3/J4) will:

3.8.1. Designate a representative to serve on the P&ISG.

3.8.2. Support and enforce the decisions of the P&ISG.

3.9. Plans and Policy Directorate (TCJ5) will:

3.9.1. Designate a representative to serve on the P&ISG.

3.9.2. Assume proponency for Joint Mobility Analysis and Modeling & Simulation functions as sanctioned by the P&ISG.

3.9.3. Support and enforce the decisions of the P&ISG.

3.10. Military Traffic Management Command (MTMC) will:

3.10.1. Designate a representative to serve on the P&ISG.

3.10.2. Support and enforce the decisions of the P&ISG.

3.11. Military Sealift Command (MSC) will:

3.11.1. Designate a representative to serve on the P&ISG.

3.11.2. Support and enforce the decisions of the P&ISG.

3.12. Air Mobility Command (AMC) will:

3.12.1. Designate a representative to serve on the P&ISG.

3.12.2. Support and enforce the decisions of the P&ISG.

3.13. Defense Courier Service (DCS) will:

3.13.1. Designate a representative to serve on the P&ISG.

3.13.2. Support and enforce the decisions of the P&ISG.

4. Internet Use:

4.1. Internet use must be work related except as indicated in paragraph 4.3. This includes all communications determined to be in the interests of the Federal Government and USTRANSCOM. Use should be appropriate in its frequency and duration and should be related to assigned tasks. USTRANSCOM employees can use the Internet resources to:

4.1.1. Obtain/exchange information to support Department of Defense (DoD) and the USTRANSCOM mission.

4.1.2. Obtain/exchange information that enhances professional skills of USTRANSCOM employees which benefits the unit and job performance within the unit.

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

4.2. Use of Internet for e-mail. E-mail may be intercepted and reviewed by third parties. Classified, operationally sensitive, or information, which if intercepted, would likely compromise future or ongoing operations or adversely reflect on DoD, will not be transmitted using unencrypted Internet e-mail.

4.3. Incidental Use. Government computers may be used to access the Internet for incidental personal purposes such as brief communications, brief Internet searches, and other uses allowed by the DoD Joint Ethics Regulation as long as such use:

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

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

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

4.3.4. Does not overburden Federal Government computing resources or communications systems or result in added costs to the Government.

4.3.5. Is not used for purposes that adversely reflect on USTRANSCOM and the Federal Government (see Attachment 3).

4.4. Prohibited Activities. Express prohibitions, to include access to, or downloading of files containing obscene or pornographic material are at Attachment 3 and shall be strictly enforced.

5. Public Access Internet Systems (USTRANSCOM, Scott AFB IL, only):

5.1. Establishing a public Internet server and homepage. Homepages will only consist of information properly cleared for public release. Hypertext links to additional public information or pointers to other public Internet sites may be utilized; however, the OPR is responsible to ensure all linked information meets the requirements of this instruction and pointers to other public sites are appropriate (e.g., a pointer to a political party site or a contractor's commercial homepage would be inappropriate).

5.2. Approval process of public releasable information. Prior to being placed on the Internet, information must be approved for public release by the following: the originating Director or DRE Chief, TCJA, TCIM, and TCPA. The USTRANSCOM Webmaster will move the originator's proposed Web page to the "approval area" within one duty day, and each reviewing office should normally process the originator's request within five duty days of receipt of the

Web page. Flow chart for the approval process for public access Internet page(s) is at Attachment 4.

5.2.1. Biographical information on other than the Directors, DRU Chiefs, or DRE Chiefs, highly technical and voluminous information should not be placed on the Internet. Directors having a USTRANSCOM mission-need which requires them to place voluminous data on the Public Access Internet System will coordinate an alternate approval system with the approving officials in paragraph 5.2. so that adequate safeguards are in place to ensure quality is maintained even though routine changes or updates may not require review. In cases of high volume (multiple continuous page changes) replacement pages can be submitted to the USTRANSCOM Webmaster for direct posting on the production server subject to spot checks (not to exceed 30 calendar days between checks) by TCIM, TCJA, and TCPA as shown in Attachment 5.

5.2.2. All information placed on the Public Access Internet System shall conform to the USTRANSCOM WWW Style Guide, USTRANSCOM Handbook 33-302.

6. Limited Access - Official Government Only Systems:

6.1. Systems which are engineered to allow access only to official Government users, to include contractors when performing tasks pursuant to a Government contract, are not considered "public release" and do not need to be reviewed by TCPA, TCIM, and TCJA prior to placement on the system. This places greater responsibility on the information provider to ensure PA, FOIA, and FOUO material is protected to the extent possible. Systems must have appropriate user registration procedures, user identification, or password controls which limit the access to a specific group(s) (e.g. only those addressees in the ".gov" or ".mil" domains).

6.2. As access by Government contractors is contemplated, no proprietary data or source selection sensitive material may be placed on these systems IAW Procurement Integrity Act, Title 41, United States Code, Section 423, as amended. Extreme care must be taken to ensure current Government contractors do not receive a competitive advantage for future acquisitions by having access to information on the limited access web pages that is not available to other competing contractors.

6.3. Limited access approval process. At USTRANSCOM, approval authority is normally at the director/DRE chief level. Directors/Chiefs of DREs may delegate approval authority at their discretion. Any information inconsistent with existing USTRANSCOM policy or proposing new policy will normally be approved by the USTRANSCOM Command Section prior to placement on the Internet. Flow chart for the approval process for limited access Internet pages is at Attachment 6.

6.4. Common-User Transportation Related Systems. All TCC WWW programs, homepages, and systems, whether public access or limited access, which provide access to operations-related data; such as, schedules for Operational Support Airlift (OSA), Special Assignment Airlift Missions (SAAMs), other scheduled channel or charter flights, or surface transportation scheduled by USTRANSCOM or its component commands, will be designed and operated to ensure that only categories of data consistent with USTRANSCOM policies are maintained. TCCs will ensure accurate data is displayed at all times and consistent with information being provided by USTRANSCOM and the other TCCs. In all cases, information which may be accessed from the Internet will be professionally presented, current, accurate, and related to USTRANSCOM's mission.

7. Restrictions at USTRANSCOM Scott AFB IL:

7.1. No software will be downloaded from any Internet resource for personal use or gain. USTRANSCOM personnel will not download commercial software or "shareware" that obligates the Government for payment.

7.2. All files that are downloaded will be scanned and cleared of viruses prior to being used on USTRANSCOM systems. Any executable programs or copyrighted material that is downloaded for possible use on USTRANSCOM computer systems will be approved through the Automated Communications Computer Systems Requirement Document (ACSRD) process prior to being loaded to avoid infringements and violation of copyrights, patents, and licensing agreements.

7.3. Anonymous File Transfer Protocol (FTP) services, other than those controlled and administered by TCJ6 and TCJ5 Joint Mobility Analysis Center (JMAC), are not allowed to be used at USTRANSCOM.

8. Security:

8.1. IAW Joint Chiefs of Staff (JCS) Joint Pub 6-03.7, DoD Directive (DoDD) 5200.28, Air Force Security Systems Instruction (AFSSI) 5102, and USTRANSCOM Regulation 205-4, TCJ6 is appointed the Designated Approval Authority (DAA) for all USTRANSCOM computer systems. For systems processing information categorized as "Secret" to "Unclassified," DAA has been further delegated to TCJ6 Operations and Security Division (TCJ6-O). The DAA approves the establishment of all WWW or Internet Web sites or homepages. See Attachment 2 for guidelines for Web site establishment.

8.2. Users are responsible for practicing good security while accessing the Internet. Anyone observing a suspected security breach must report it immediately to their security manager,

TCJ6-OS, or Force Protection Branch (TCFP-O). Security managers will make recommendations for formal investigations to TCJ6-O and TCFP-O.

8.3. The limited access Web sites must be secured from publicly accessible networks by a firewall or a filtering router which has policies prohibiting all protocols not necessary for business operation. The topology of the network must be provided to TCJ6-O for approval.

STEPHEN E. KELLEY
Brigadier General, USAF
Director, Command, Control, Communications
and Computer Systems

6 Attachments
1. Glossary of References, Abbreviations, Acronyms, and Terms
2. USTRANSCOM's Guidelines for Web Site Establishment
3. Prohibited Use of Internet Services
4. Flow Chart - WWW Public Access Page Approval Process
5. Flow Chart - WWW Public Access Page (High Volume) Approval Process
6. Flow Chart - WWW Limited Access Page Approval Process

DISTRIBUTION: X (TCCC-P, TCCC-Q, TCFP, TCIG, TCIM, TCJA, TCPA, TCRC - 1 each; GPMRC, TCJ8, TCSG - 2 each; JTCC, TCJ5 - 4 each; TCDC-JS, TCJ1, TCJ2, TCJ6 - 5 each; TCJ3/J4 - 12; AMC/SC, Defense Courier Service (DCS/CC), Building P830, Chisholm Avenue, Ft Meade MD 20755-5370, MTMC/MTIM-P, 5611 Columbia Pike, Falls Church VA 22041-5050, MSC/N6/N0021, Washington Navy Yard, 901 M Street SE, Washington DC 20398-5540 - 12 each).

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

Section A -- References

Freedom of Information Act, Title 5, United States Code, section 552, as amended.

Procurement Integrity Act, Title 41, United States Code, section 423 et seq.

Deputy Secretary of Defense Policy Memorandum "Clearance Procedures for Making Electronic Information Available to the Public," 17 Feb 95.

DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs).

DoD Directive 5230.9, Clearance of DoD Information for Public Release.

DoD 5500.7-R, Joint Ethics Regulation.

Joint Pub 6-03.7, Security Policy for the WWMCCS Intercomputer Network.

USTRANSCOM Policy Directive 33-3, USTRANSCOM Internet Access and Use

USTRANSCOM Instruction 37-8, USTRANSCOM Freedom of Information Act Program.

USTRANSCOMR 205-4, USTRANSCOM Computer Security Policy.

AFSSI 5102, Computer Security (COMPUSEC) for Operational Systems.

Section B- -Abbreviations and Acronyms

ACSRD - Automated Communications Computer Systems Requirement Document

ADP - Automated Data Processing

AFSSI - Air Force Security Systems Instruction

AMC - Air Mobility Command

BBS - Bulletin Board Systems

CIO - Chief Information Officer

CXE - Client Executable Evaluator

DAA - Designated Approval Authority

DoD - Department of Defense

DRE - Direct Reporting Element

DRU - Direct Reporting Unit

e-mail - Electronic mail

FACCSM - Functional Area Communications-Computer System Manager

FOIA - Freedom of Information Act

FOUO - For Official Use Only

FTP - File Transfer Protocol

HTML - Hypertext Markup Language

HTTP - Hypertext Transfer Protocol

INFOSEC - Information Security

IP - Internet Protocol

MSC - Military Sealift Command

MTMC - Military Traffic Management Command

NIPRNet - Non-Secret Internet Protocol Network

OS - Operating System

OSA - Operational Support Airlift

OPR - Office of Primary Responsibility

PA - Privacy Act

P&ISG - Policy and Implementation Steering Group

POC - Point of Contact

URL - Uniform Resource Locator

USCINCTRANS - Commander in Chief, USTRANSCOM

USTRANSCOM - United States Transportation Command

SAAMs - Special Assignment Airlift Missions

TCC - Transportation Component Command

WWW - World Wide Web

24 X 7 - Twenty four hours a day, seven days a week

Section C- -Terms

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

External Server. An Internet host computer system which is accessible by the general public without user access controls; such as, user ids and passwords.

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

Gatekeeper. Refers to the points of contact for World Wide Web activities for each directorate/DRE.

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

Internet. A collection of a worldwide "network of networks" that uses the transmission control protocol/interface protocol (TCP/IP) for communications. The Internet includes resources that span academia, business, Government, and personal interests.

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

Public Information. Public information is official information posted on the USTRANSCOM or TCC homepages that have been approved for public release by appropriate authorities in accordance with listed references. This type of information is made available with no controls to limit access by Internet users. Normally, all public information will be distributed by the Public Affairs Office.

Shareware. Copyrighted software that has been developed and placed in the public domain or in general circulation on increase public use. The developer of such software usually requests a nominal fee using the honor system for the software and its future updates. Such "offers" may not be accepted by Government personnel on behalf of the Government without proper authorization.

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

Uniform Resource Locator (URL). The standard address and address format for a resource on the Internet. An example is: http://www.transcom.safb.af.mil.

Webmaster. The TCJ6 World Wide Web administrator.

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

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

USTRANSCOM'S GUIDELINES FOR WEB SITE ESTABLISHMENT

VERSION 1

A2.1. The web site must be secured from publicly accessible networks by a firewall or a filtering router which has policies prohibiting all protocols not necessary for business operation. The topology of the network must be provided to TCJ6-O for approval.

A2.2. The Domain Naming Service entries for all Universal Resource Locator (URL) referenced systems comprising the site must be verifiable and, where possible, resolvable, both as a Fully Qualified Domain Name and as an Internet Protocol (IP) address. All USTRANSCOM servers will be part of the "transcom.mil" domain.

A2.3. Logging of the connecting IP addresses, date and time, pages accessed, date and time of each secure connect and disconnect, and denials of access/unauthorized access attempts must be maintained for users accessing the certified web server.

A2.4. A generally accepted encryption/security mechanism (i.e., Secure Socket Layer) must be used for sensitive data transmissions. A risk assessment--balance the risk of unauthorized disclosure against level of protection and cost--is required if privacy act data, i.e., social security numbers, are transmitted.

A2.5. Each web site must designate an individual who has read, understood, tested, and reviewed the site's Common Gateway Interface scripts and can verify they conform to USTRANSCOM security practices.

A2.6. Each web server must designate a Client Executable Evaluator (CXE) who examines and evaluates JAVA and other client executable applications. The CXE must be able to verify the origins of all applications to insure they have no Trojan horses or malicious codes.

A2.7. Pages containing or accepting sensitive data must be non-cacheable.

A2.8. The web server must meet various physical and logical security checks such as physical location, locks, access controls, backup procedures, emergency contact, etc.

A2.9. The operating system (OS) of the server must be documented to certify that the software came from a known, reputable vendor or site and that current software patches are in place.

A2.10. The web server software shall be installed and configured in accordance with the best common security practices as defined by TCJ6-OS and the configuration guidelines common to USTRANSCOM and defined by TCJ6-OMW. This will require granting TCJ6-OS and TCJ6-OMW access to perform periodic inspections.

A2.11. The OS of the server must be resistant to penetration attempts from external and internal hosts. For example: automated hacker tool kit attack such as Satan and password sniffer attack.

A2.12. The administration of the OS and the web server will be reviewed to verify compliance with USTRANSCOM security practices.

A2.13. Database servers will not be run on the same system on which the web server is operating. Any "back-end" transactions processes must be documented and available for review.

Note: Criteria are based on the recommendations of the National Computer Security Association and will be updated on an as needed basis in order to ensure that USTRANSCOM web sites are as secure as possible in the dynamic, ever changing Internet environment.

PROHIBITED USE OF INTERNET SERVICES

A3.1. The use of Internet services in the following types of activities is specifically prohibited:

A3.1.1. Illegal, fraudulent, or malicious activities.

A3.1.2. Partisan political activity, political or religious lobbying or advocacy, or activities on behalf of organizations having no affiliation with USTRANSCOM or DoD.

A3.1.3. Activities whose purposes are for personal or commercial financial gain. These activities may include chain letters, solicitation of business or services, and sales of personal property.

A3.1.4. Unauthorized fundraising or similar activities, whether for commercial, personal, or charitable purposes. Official morale, welfare, recreation, officer and enlisted aid activities may be authorized.

A3.1.5. Accessing, storing, processing, displaying, transmitting or distributing offensive, sexually explicit, or obscene material such as pornography and hate literature.

A3.1.6. Storing, processing, or distributing classified, proprietary, or other sensitive information on a computer or network not explicitly approved for such processing, storage, or distribution.

A3.1.7. Annoying or harassing another person, e.g., by sending or displaying uninvited e-mail of a personal nature or by using lewd or offensive language in an e-mail message.

A3.1.8. Using another person's account or identity without his or her explicit permission, e.g., by forging e-mail, except when authorized by proper authority.

A3.1.9. Viewing, damaging, or deleting files or communications belonging to others without permission or authorization by proper authority. ***NOTE:*** *There is no expectation of privacy when using USTRANSCOM Government computers and equipment. Personal files should not be stored on Government systems.*

A3.1.10. Attempting to circumvent or defeat security or auditing systems without prior authorization and other than as part of legitimate system testing or security research.

A3.1.11. Obtaining, installing, storing, or using software obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

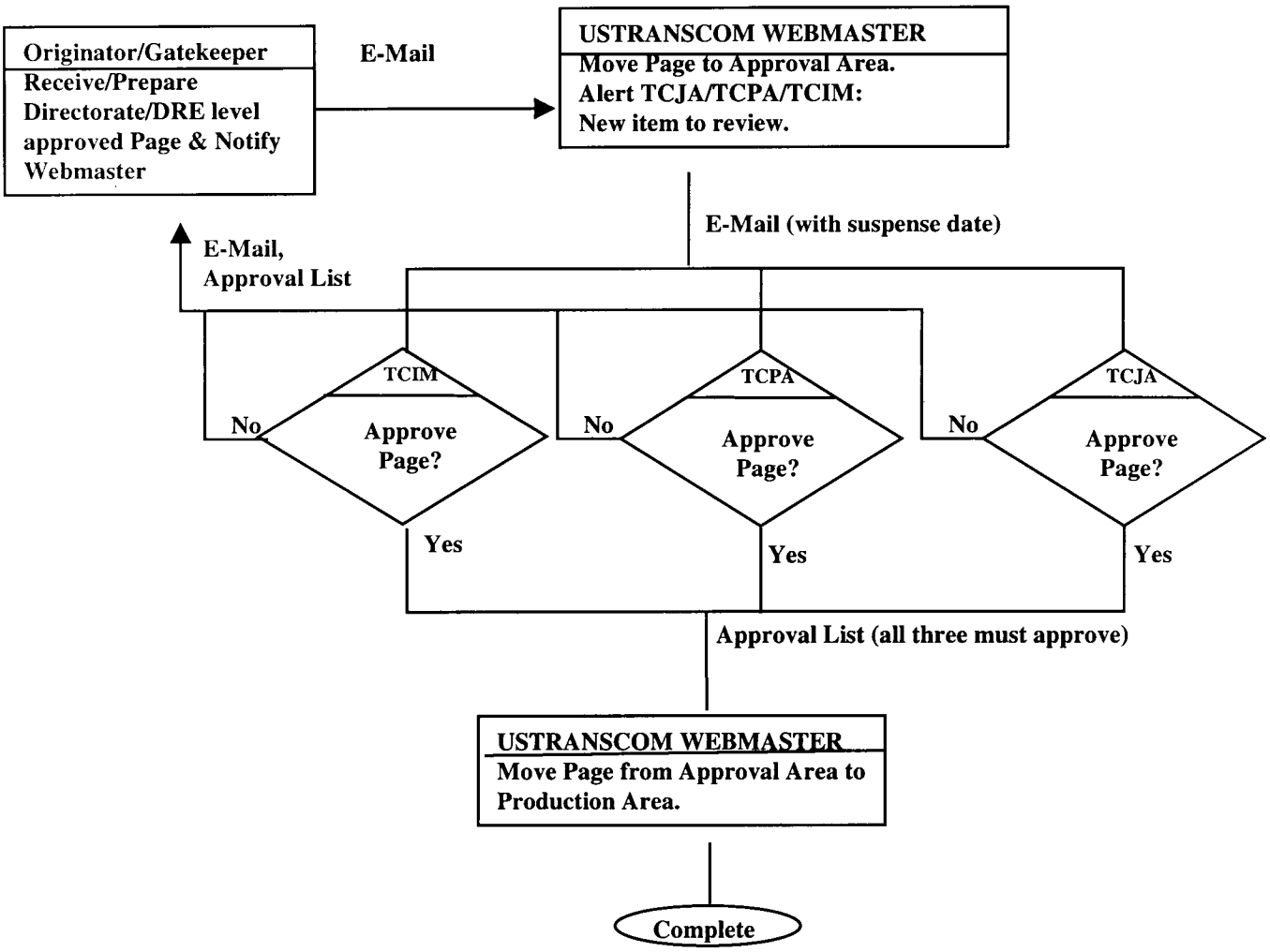
A3.1.12. Permitting any unauthorized person to access a U.S. Government-owned system.

A3.1.13. Modifying or altering the operating system or system configuration without first obtaining permission from the owner or administrator of that system.

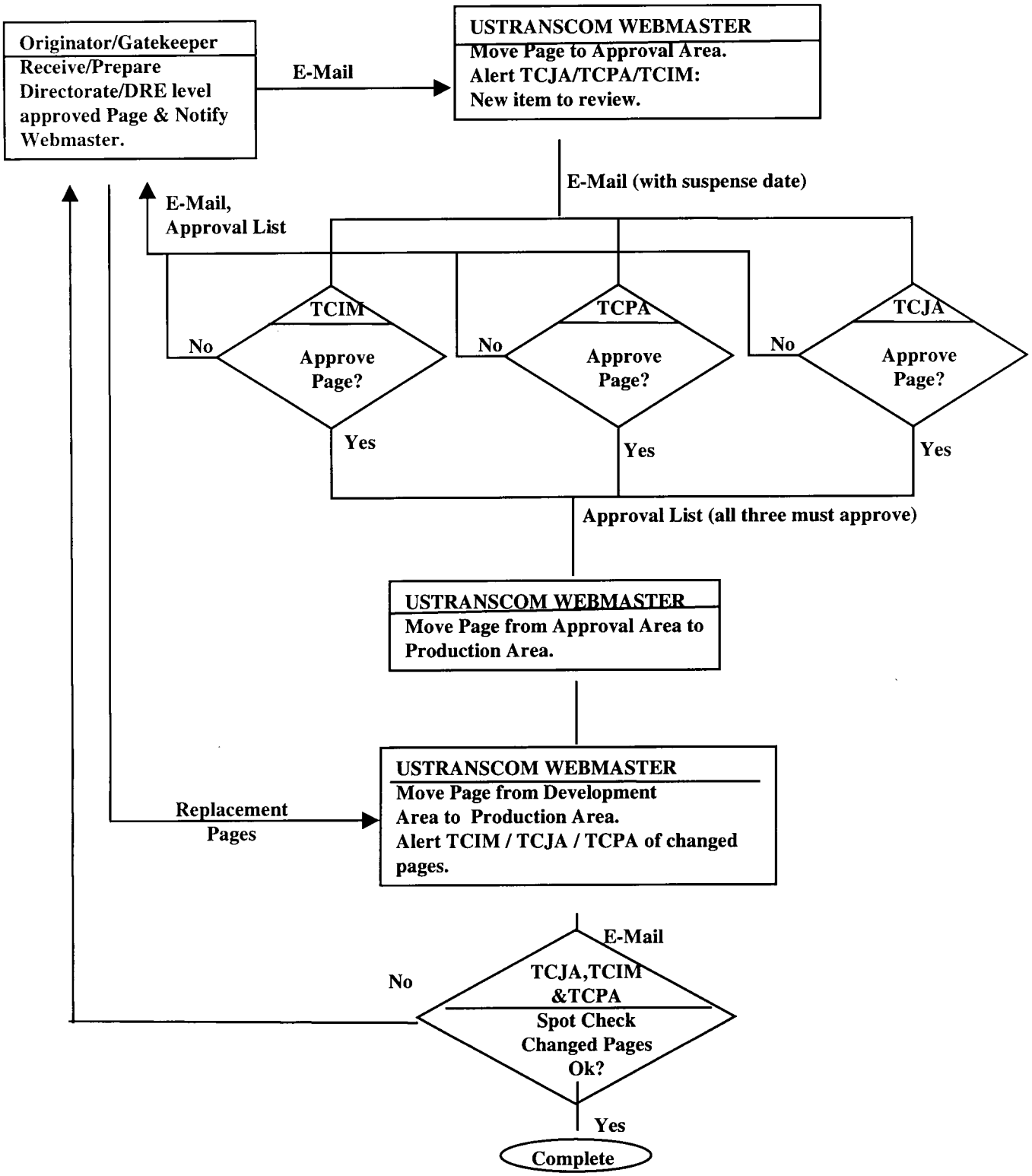
A3.1.14. Using e-mail to circumvent or bypass the normal chain of command for official actions.

A3.2. Violation of the listed prohibitions may result in adverse administrative or other disciplinary action being taken against the individual. Such actions may include proceedings pursuant to the Uniform Code of Military Justice, non-judicial punishments, personnel disciplinary actions, and adverse comments/ratings on performance appraisals.

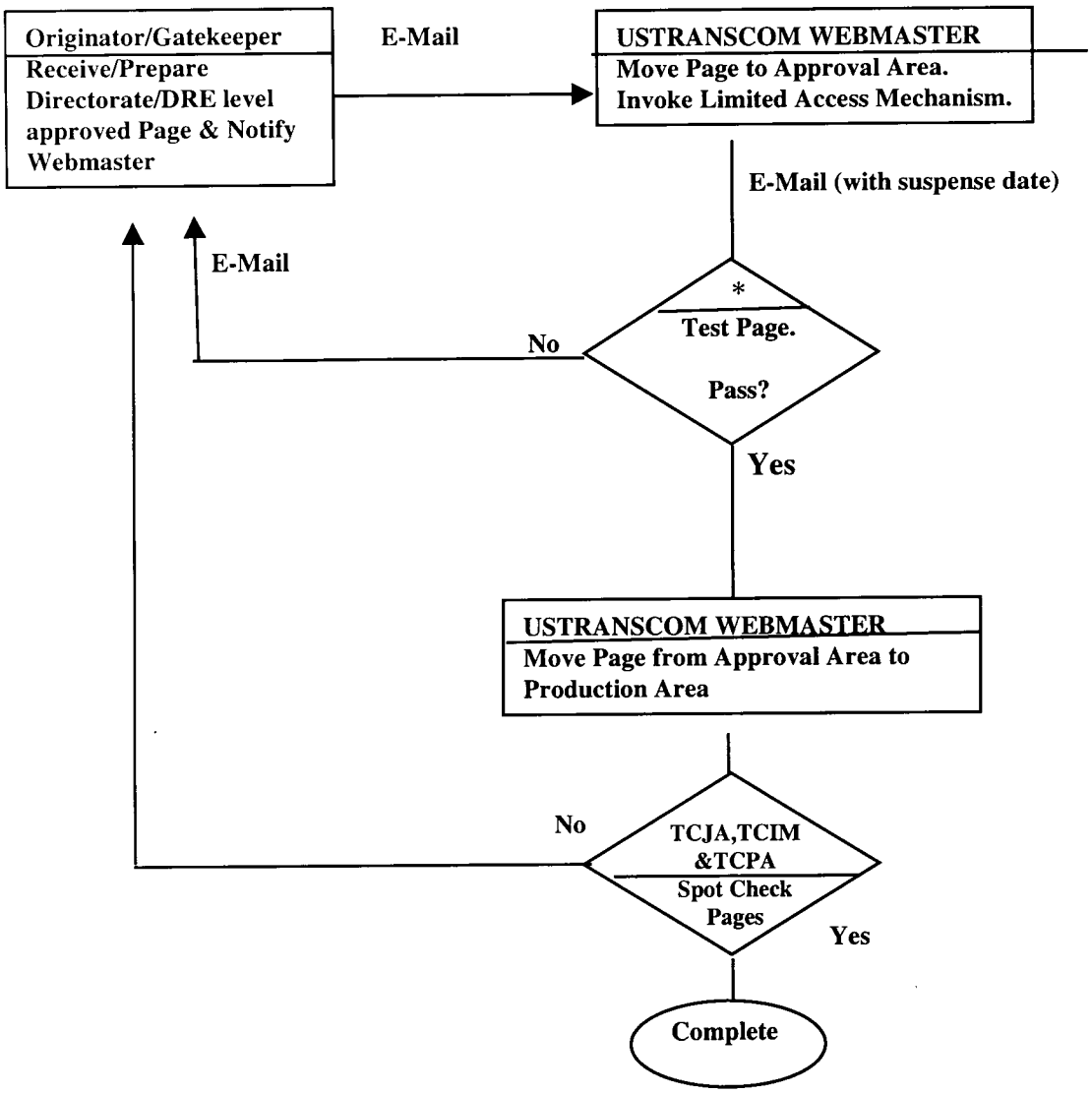
WWW Public Access Page Approval Process



WWW Public Access Page Approval Process (High Volume)



WWW Limited Access Page Approval Process



* Page should be tested by a representative operational community (beta test).