



Communications and Information

MANAGEMENT OF PORTALS AND WEB SITES

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available electronically on the USTRANSCOM electronic library.

RELEASABILITY: There are no releasability restrictions on this publication

OPR: TCJ6-OM

Approved By: TCJ6 (Brig Gen Gregory Touhill, USAF)

Supersedes: USTRANSCOMI 33-3, 21 Sep 2007

Pages: 10

Distribution: e-Publishing

This instruction establishes policies and procedures for the use and management of web portals, sites, and applications within United States Transportation Command (USTRANSCOM). It applies to all personnel, including contractors, assigned or attached to USTRANSCOM. Compliance is mandatory. Failure by military personnel to observe the prohibitions and mandatory provisions of this instruction is a violation of Article 92, Uniform Code of Military Justice. Violations by civilian employees may result in disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by contractor personnel may result in denied access to systems, contractual remedies against the contractor, or debarment from the installation. This instruction does not establish any rights or entitlements. The use of a name or mark of any specific manufacturer, commercial product, commodity, or service in the publication does not imply endorsement by USTRANSCOM. Refer recommended changes and questions about this instruction to the office of primary responsibility using Air Force Form 847, *Recommendation for Change of Publication*. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with USTRANSCOM Instruction 33-32, *USTRANSCOM Records Management Program*.

SUMMARY OF REVISIONS

This instruction defines new policies and procedures for managing web content and documents published to portals and web sites. It redefines staff responsibilities in the publishing process, updates references, and defines all acronyms.

1. Policy and Procedures:

1.1. Policy:

1.1.1. Unrestricted Access Internet Protocol Router Network (NIPRNET) Portals and Web Sites:

1.1.1.1. Public access portals and web sites are those open to the public internet without restriction. They shall contain only unclassified information that has been properly reviewed and approved for public release. They will not contain classified information, unclassified information that is For Official Use Only, Privacy Act, or sensitive but unclassified data.

1.1.1.1.1. Content will be prepared by appointed USTRANSCOM organizational gatekeepers and subject matter experts (SME), and submitted for release and publication by the organizational gatekeeper.

1.1.1.1.2. All content submitted for public release will be reviewed within the context of operational security (OPSEC), Freedom of Information Act, Privacy Act, Section 508 of the Rehabilitation Act compliance for access by individuals with disabilities, other legal considerations, technical standards, and suitability for public release.

1.1.1.2. Restricted access portals and web sites use an authentication process to control access based on community membership, programs, or other criteria as defined by the functional manager. These sites will contain only unclassified information.

1.1.1.2.1. Content may be prepared by appointed USTRANSCOM organizational gatekeepers or SMEs and published directly where an interface is available. Content that cannot be published directly will be submitted for publication to the Web Development Team (Customer Support Section of Web Shop of Command, Control, Communications and Computer Systems Directorate (TCJ6)) by the gatekeeper.

1.1.1.2.2. Gatekeepers and SMEs will review all content prior to publication, or submission to the Web Development Team for publication, within the context of OPSEC, 508 compliance, and defined technical standards.

1.1.2. Secret Internet Protocol Router Network (SIPRNET) portals and web sites:

1.1.2.1. Content will be prepared by appointed USTRANSCOM organizational gatekeepers and SMEs and will meet the same 508 compliance and technical standards as NIPRNET content.

1.1.2.2. Prior to publication, SIPRNET documents will be reviewed by the Foreign Disclosure Officer (FDO) or Foreign Disclosure Representatives (FDR) to determine releasability to coalition partners.

1.1.2.3. In most cases, gatekeepers and SMEs will be able to publish directly onto SIPRNET portals and web sites.

1.1.3. Auditing and meta-data collection:

1.1.3.1. Auditing mechanisms will be implemented by the Web Development Team to ensure full attribution for all publishing transactions—upload, change, and delete. This will be implemented first on the SIPRNET and then the NIPRNET.

1.1.3.2. Tools implemented to provide the auditing mechanism will also provide the ability to capture meta-data for each document published to enable robust web content management.

1.1.4. Acceptable content for portal and web site publication. The following electronic file formats are authorized for publication on the command portals and web sites: static Hypertext

Markup Language (HTML), Microsoft Office products (.doc, .ppt, and .xls), Adobe Acrobat files (.pdf), Joint Photographic Experts Group images (.jpg), Tagged Image File Format (.tif or .tiff) and Bitmap (.bmp). Gatekeepers and SMEs are not permitted to publish dynamic content - JavaScript, Cold Fusion, Java Server pages, etc. User-developed applications will not be accepted for hosting on sites managed by the Web Development Team.

1.1.5. Public portal and web site review and approval. Command reviewing authorities for publication of content to public portal and web sites are: Public Affairs, Staff Judge Advocate, Information Operations (TCJ3-SI), and Freedom Office.

1.1.5.1. Public Affairs is the final approval authority for publication to the command portals and web sites.

1.1.5.2. In addition, a technical review will be performed by the Web Development Team prior to publication.

1.2. Procedures:

1.2.1. Preparing for publication. Web content management begins by defining ownership of all published information. Ownership begins with the originating SME developing new information for sharing with USTRANSCOM elements and customers. This information may take the form of documents, PowerPoint presentations, spreadsheets, etc. Prior to submitting information for publishing onto a USTRANSCOM network (NIPRNET or SIPRNET), the originating SME, gatekeepers and designated users with publication privileges shall review documents and content to ensure the following:

1.2.1.1. Content being published is allowed on the intended host system.

1.2.1.2. Classified material is properly marked in accordance with Department of Defense (DOD) 5200.1PH, *DOD Guide to Marking Classified Documents*, and USTRANSCOM Handbook 31-10, *USTRANSCOM Security Classification Guide*.

1.2.1.3. Special handling instructions are properly indicated and marked in accordance with DOD directives.

1.2.1.4. Classified information has been reviewed and approved for publication by the organizational FDR.

1.2.2. Publishing to public access portals and web sites:

1.2.2.1. Only organizational gatekeepers may forward content for publication on the public access systems. This is accomplished when the organizational gatekeeper submits a gatekeeper request to the Web Development Team to publish a document.

1.2.2.2. Upon receipt of a Gatekeeper Request, the Web Development Team will review the document or content for technical compliance and obvious OPSEC violations.

1.2.2.3. Following a successful review by the Web Development Team, the document or content will be placed into the Public Approval Process for review.

1.2.2.4. Once reviewing authorities complete their review, the document or content will either be published if approved or returned to the gatekeeper for further action.

1.2.3. Direct publishing to restricted SIPRNET and NIPRNET systems:

1.2.3.1. Gatekeepers, SMEs, and designated users may publish directly into most restricted systems via general purpose publishing interfaces provided by the Web Development Team or application-specific publishing mechanisms. Several publishing mechanisms are available to USTRANSCOM users and it is beyond the scope of this document to provide specific information on their use.

1.2.3.2. Auditing information will be automatically collected for each publishing transaction to ensure proper identification of the publisher, establish responsibility, and ensure attribution and non-repudiation.

1.2.3.3. Publishers must provide requested meta-data to complete a publishing transaction. Failing to provide such information will automatically abort the publication request.

1.2.3.4. Organization FDRs will review all classified documents and content to be published on SIPRNET systems for potential foreign disclosure issues.

1.2.3.5. Additional information may be required by the target host environment prior to publication. In these cases, failure to provide such certification will automatically abort the publication request.

2. Roles and Responsibilities:

2.1. USTRANSCOM TCJ6 is responsible for the security and administration of the command's unclassified and classified web servers.

2.2. Web Development Team (Systems Operations Branch (TCJ6-OM)) will:

2.2.1. Develop and maintain USTRANSCOM's Internet systems in conjunction with TCJ6-OM.

2.2.2. Use strict stylistic controls to ensure a consistent and professional image is presented on all USTRANSCOM web sites.

2.2.3. Maintain an Internet development environment and provide assistance to and ensure training of USTRANSCOM gatekeepers.

2.2.4. Investigate emerging Internet technologies in conjunction with USTRANSCOM Test Facility, to maintain technical currency of software and hardware.

2.3. Information Owner (Directorate/Command Support Group) will:

2.3.1. Ensure publicly accessible web pages and common folders consist of information that is properly cleared for public release in accordance with DOD Directive 8500.01E, *Information Assurance*, and all other official security and classification guidance. Directors may delegate content approval to the lowest capable level of responsibility in their organizations. For example, some directorates may feel it appropriate to delegate their authority to the branch chief level because that is the lowest organizational level with a gatekeeper.

2.3.2. Identify gatekeepers through an appointment letter. Appointing official will ensure that the appointee receives gatekeeper training prior to assuming duties. Appointing officials will prepare an appointment letter designating what networks and offices the assignee will support. Before appointing contractors as gatekeepers, appointing officials must review their contract duties with the contracting officer or contracting officer representative. Contractors may not be gatekeepers if their contracts do not cover such duties. Appointing officials should contact Staff Judge Advocate for guidance. All appointment letters must be reviewed semiannually or whenever a gatekeeper departs or is reassigned. Gatekeepers should be a United States citizen. Non-United States citizens must be vetted and approved by the USTRANSCOM FDO and will have limited capabilities on what they can post.

2.4. Gatekeepers:

2.4.1. Organizational gatekeepers are the organizational point of contact for all organizational content published on USTRANSCOM SIPRNET and NIPRNET portals and web sites. They prepare and manage content for their branch/division/directorate and publish the content on USTRANSCOM portals and web sites.

2.4.2. Gatekeepers are responsible for maintaining currency and accuracy of information placed on their site. A quarterly review by all gatekeepers will be conducted with SMEs to determine if content is current or requires deletion. A review/deletion of content will be directed by the Web Development Team, as required. Notification of the review/deletion will be done via email to all gatekeepers.

2.4.3. Gatekeepers will be responsible for ensuring content complies with standards for publication on both NIPRNET and SIPRNET systems.

2.4.4. Prior to assuming gatekeeper duties, training is mandatory with an emphasis on education and familiarization for OPSEC, foreign disclosure, Section 508 compliance, and public affairs issues. Gatekeeper training is scheduled through the respective Directorate/Command Support Group training officials.

2.4.5. Following training, gatekeepers shall access and use instructional and reference material located on the NIPRNET. Included for use are checklists for release requests, updates, Section 508 of the Rehabilitation Act compliancy methods and guidance on removal of information. The Web Development Team will provide individual assistance to all gatekeepers, as needed.

Semiannual review of all gatekeeper letters will be conducted by the Web Development Team. Gatekeepers and Appointing Officials will be notified of the status of the appointment letters.

2.5. FDR. Directors shall appoint, in writing, an FDR to review all documents and information to be published on SIPRNET portals and web sites for releasability to coalition partners. An individual is only considered an FDR after they receive required training by the USTRANSCOM FDO and will not be tasked to perform duties as an organizational gatekeeper. An FDR must be a United States citizen.

2.6. TCJ3-SI. TCJ3-SI is responsible for the command's Critical Information List and overall command OPSEC program. TCJ3-SI will conduct semiannual training classes to provide OPSEC guidance to gatekeepers, SMEs, and information owners, as necessary.

2.7. FDO. The USTRANSCOM FDO is responsible for training gatekeepers and FDRs on foreign disclosure of information. The FDO will provide, at a minimum, semiannual training to gatekeepers, SMEs, and information owners on proper classification and releasability of information.

3. Security. In accordance with DOD Directive 8500.01E, TCJ6 has been appointed the Designated Approval Authority (DAA) for all USTRANSCOM computer systems. The DAA approves establishment of USTRANSCOM web sites. USTRANSCOM Information Assurance Manager will establish and implement security measures to protect information on command web portals and web sites.

GREGORY J. TOUHILL
Brigadier General, USAF
Director, Command, Control, Communications
and Computer Systems

2 Attachments:

1. Glossary of References, Abbreviations, Acronyms, and Terms
2. USTRANSCOM Web Site Configuration Guidance

Attachment 1

GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS

Section A—References

Federal Rehabilitation Act, Section 508
 Department of Defense (DOD) 5200.1PH, *DOD Guide to Marking Classified Documents*
 DOD Directive 8500.01E, *Information Assurance*
 USTRANSCOM Handbook 31-10, *USTRANSCOM Security Classification Guide*

Section B—Abbreviations and Acronyms

DAA – Designated Approval Authority
 DOD - Department of Defense
 FDO - Foreign Disclosure Officer
 FDR - Foreign Disclosure Representative
 HTML - Hypertext Markup Language
 NIPRNET - Unclassified but Sensitive Internet Protocol Router Network
 OPSEC - Operations Security
 SIPRNET - Secret Internet Protocol Router Network
 SME - Subject Matter Expert
 TCJ3-SI – Operations and Plans Directorate, Information Operations Division
 TCJ6 - Command, Control, Communications and Computer Systems Directorate
 TCJ6-OM – TCJ6 Systems Operations Branch
 USTRANSCOM - United States Transportation Command

Section C - Terms

Not Used

Attachment 2

USTRANSCOM Web Site Configuration Guidance

A2.1. Web Server Configuration Criteria. Users should first take advantage of USTRANSCOM's established web capability before considering establishing a new web server. Where existing capabilities are inadequate, new web servers can be established after requirements have been approved through the Cyberspace Infrastructure Planning System (CIPS) process. All USTRANSCOM web servers must meet the following requirements.

A2.1.1. The web site must be secured from publicly accessible networks by a stateful packet inspection firewall which has policies prohibiting protocols not necessary for business operation. The placement of the web server on the network must be reviewed and approved by TCJ6-O prior to installation.

A2.1.2. The Domain Naming Service (DNS) 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 "ustrancom.mil" domain.

A2.1.3. All mobile code must comply with the DOD Mobile Code Policy.

A2.1.4. Logging within the web server and web application must conform to USTRANSCOM's auditing policy.

A2.1.5. A generally accepted encryption/security mechanism (i.e., Secure Socket Layer (SSL)) 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 is transmitted.

A2.1.6. If the site requires a certificate, a DOD server certificate must be used. Demo or vendor-provided certificates will not be used.

A2.1.7. Pages containing or accepting sensitive data must be non-cacheable.

A2.1.8. All pages containing sensitive material must use two factor authentications. The current command standard is use of the Common Access Card (CAC).

A2.1.9. Database servers will not be run on the same system on which the web server is operating. Any back-end transaction processes must be documented and available for review. All communications between the web server and the database server must be secure and logged.

A2.1.10. No development should be done on a production server, and there must be strict separation between development and production system.

A2.1.11. Public and restricted applications cannot reside on the same system.

A2.1.12. Multiple public or multiple restricted applications can reside on the same system provided they are segmented appropriately.

A2.1.13. Data sources such as a database or file server must not be shared between restricted and public applications. This includes schemas, views, etc.

A2.1.14. Any system accounts used for system to system communication (e.g., database connections) shall not be shared between systems or applications. This prevents a compromised system from providing access to another system.

A2.1.15. Administration of the web server and application will not be done through the standard user interface. A unique interface on a different port with strong Access Control Lists (ACL) shall be used.

A2.1.16. The web server must meet various physical and logical security checks such as physical location, locks, access controls, backup procedures, emergency contact, etc.

A2.1.17. The Operating System (OS) of the server must be documented to certify that the software came from a known, reputable vendor or site. The OS must be configured to USTRANSCOM guidelines and have current software patches in place.

A2.1.18. The web server software shall be installed and configured in accordance with the best common security practices as defined by TCJ6-OIP and the configuration guidelines common to USTRANSCOM. Any web application is subject to security assessment and/or source code review upon request by TCJ6-OIP.

A2.1.18.1. File permissions of the server should follow a strict need to know policy for both the document root (where HTML documents are stored) and the server root (where log and configuration files are kept).

A2.1.18.2. A minimal system install must be performed. Only software and application modules that are required for the operation of the server are to be installed.

A2.1.18.2.1. All demo/default documentation-type files must be removed.

A2.1.18.2.2. All operating system services and web server optional features that are not required should be disabled. Examples of potentially dangerous web server optional features include: automatic directory listings, symbolic link following, and server side includes.

A2.1.18.3. Web server cannot be run with elevated privileges. Servers can be launched as root but must have the capability and be configured to run child processes as an unprivileged user.

A2.1.18.4. All user input must be validated on the server before any action is taken with it to prevent unauthorized access to system functionality or data. Invalid data attempts must be logged.

A2.1.18.4.1. All characters that are part of HTML tags or entities ('<', '>', '&', etc.) should be removed from user input before it is presented back to a web-site visitor to prevent Cross Site Scripting (XSS) attacks.

A2.1.18.4.2. User form input that is submitted that will be used as part of a SQL database query must be validated for format and content before it is passed to the database. SQL injection vulnerabilities exist when invalidated user input that contains SQL commands is passed through a web-form to a back-end database.

A2.1.18.5. The World Wide Web Security Frequently Asked Questions is located at <http://www.w3.org/Security/Faq/>. It provides the why, and some how, concerning best common security practices.

A2.1.19. The administration of the Operating System (OS) and the web server will be reviewed to verify compliance with USTRANSCOM security practices.

A2.1.20. All servers to be connected to the Internet must have formal, written accreditation from the DAA or TCJ6-O. Guidance and assistance on completing the accreditation process are available from TCJ6-OIP.

A2.2. USTRANSCOM Web Server Baseline Standards. USTRANSCOM's general purpose web architecture is designed to be flexible, scalable, and supportable using readily available approved commercial hardware and software components. A three tier model is used to provide functionality, i.e., Apache Server, Cold Fusion Application Server, and an Oracle database. OS specific programs and scripting and proprietary solutions are avoided to ensure, as much as possible, long-term supportability. Systems developed that do not conform to the following specifications may not be supportable at USTRANSCOM.

A2.2.1. Hardware, Software, and Operating System. Must be supportable by the TCJ6-OM.

A2.2.2. Database Server. Must be supportable by the Database Administrations teams, TCJ6-OM.

** 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.*