Headquarters	**United States Forces Korea**
United States Forces Korea	**Regulation 25-5**
Unit #15237	
APO AP 96205-5237	

13 August 2009

Information Management

UNITED STATES FORCES KOREA PUBLIC ACCESS WORLD WIDE WEB

---

*This regulation supersedes USFK Regulation 25-5, 6 April 1999.

For the Commander:

JOSEPH F. FIL, Jr.
Lieutenant General, USA
Chief of Staff

Official:

GARRIE BARNES
Chief of Publications and
Records Management

Summary. To provide governing content and maintenance of the United States Forces Korea (USFK) public access World Wide Web (WWW) information services.

Summary of Change. This document has been substantially changed. A full review of contents is required.

Applicability.

   a. This regulation applies to all organizations, units, agencies and/or personnel assigned to USFK.

   b. This regulation applies only to USFK World Wide Web (WWW) information services that are unclassified and freely accessible to the public. This regulation does not cover classified and limited access WWW services such as the Eighth United States Army (8th Army) Intranet portal and similar Intranet services.

Supplementation. Supplementation of this regulation and issuance of command and local forms is prohibited unless prior approval is obtained from HQ USFK, PAO, Unit #15237, APO AP 96204-0042.

Forms. USFK forms are available on www.usfk.mil under Publications.

Records Management. Records created as a result of processes prescribed by this regulation must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are available on the Army Records Information System website at https://www.arims.army.mil.

Suggested Improvements. The proponent of this regulation is HQ USFK, PAO. Users are invited to send comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) to the HQ USFK, PAO, Unit #15237, APO AP 96204-0042.

Distribution. Electronic media only (EMO).

CONTENTS

Chapter 1
General, *page 4*

Chapter 2
Policies and Procedures, *page 7*

Appendices, *page 11*

Glossary, *page 21*

Chapter 1
General

1-1. Purpose
To provide governing content and maintenance of the USFK public access Internet information services on USFK.mil.

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

1-3. Explanation of Acronyms, Abbreviations and Terms
 Acronyms and abbreviations used in this regulation are explained in the Acronyms and Abbreviations Section.

1-4. Background
The Internet, in particular the World Wide Web, offers an unprecedented opportunity for the USFK to communicate messages and information to the global Internet community. With this opportunity also comes new challenges. This regulation outlines USFK policy for providing information to the public via the public access World Wide Web information service.

1-5. Responsibilities

   a. General:

      (1) USFK PA will manage and operate the USFK public access information service in accordance with (IAW) applicable Department of Defense (DOD) policy and this regulation. Commanders, directors, organization and special staff heads will contribute information to, and participate in, the development of the World Wide Web service.

      (2) All Organizations and Staff must comply with the policy as set forth in this memorandum no more than 45 days from the date of its release.

   b. The USFK PA will:

      (1) Perform necessary coordination with HQ USFK organizations and staff offices to ensure the credibility and public release-ability of material posted on the public access World Wide Web information service.

      (2) Act as the final approval authority for format, presentation, function and aesthetics of all information and multimedia posted on the public access information service and related social networking and media sharing sites including, but not limited to text, photographs, graphic art elements, videos and any other visual or audio media.

      (3) Ensure compliance with content aspects of the reference and other pertinent DOD instructions and directives.

      (4) Register the USFK public access World Wide Web information service with the Government Information Locator Service (GILS).

      (5) Draft and maintain privacy, security and exit notices as required by the reference.

(6) Conduct initial review and/or research any reports of information which, for any reason, appears to be classified, sensitive, or for official use only on the public access World Wide Web information service. If deemed necessary for further action, refer to appropriate military intelligence or military law enforcement agency.

(7) Oversee Security and Policy review process for material submitted for posting on the USFK public accessible site.

(8) Conduct initial review and/or research any reports of information posted, for any reason, appears to be inappropriate for a public access information service. If deemed necessary for further review, refer to command Operations Security (OPSEC) manager.

(9) Notify unit, agency, in writing, of outcome of review process.

(10) Return material to unit for correction/compliance with reviewers' required changes.

NOTE: PA will make minor corrections on items submitted in electronic formats.

(11) Post information to USFK site.

(12) Advise and assist Directors, Special Staff and Commanders in the use of the public access WWW information service as a means to communicate to the public.

(13) Ensure Directors, Special Staff and Commanders provide a Web Content Manager position or title, phone number, and organizational email address to be posted on their web pages.

(14) Maintain a list of Web Content Managers and their respective webpages for information.

c. **The USFK Web Developer will**:

(1) Maintain overall responsibility for hardware, software, network connections, system security, and system integrity of the public access World Wide Web information service.

(2) Provide technical support consistent with existing communication responsibilities.

(3) Provide representation to regularly scheduled meetings to provide technical expertise and discuss current status and future development of the public access information service.

(4) Ensure compliance with technical aspects of the reference and other pertinent DOD instructions and directives.

(5) Provide technical support and secure configuration of the USFK Internet server.

d. **The USFK J2 will**:

(1) Have overall responsibility for Information Security within the scope of applicable DOD regulations, while ensuring that the primary PA mission requirements of public access information services are met.

(2) Coordinate the inquiry/investigation of any reports of information, which appears to be classified, on the public access World Wide Web Information Service.

e. The USFK J39 will:

(1) Have overall responsibility for Operations Security (OPSEC) within the scope of applicable DoD and USFK regulations, while ensuring that the primary PA mission requirements of public access information service are met.

(2) Coordinate risk assessments of any reports of information, which appear to be Sensitive Information; to include USFK critical information, sensitive but unclassified information, For Official Use Only (FOUO) information; and Personally Identifiable Information (PII) discovered on any USFK or subordinate unit publicly accessible site.

(3) As required, assist PA and unit OPSEC officers with information review prior to posting and during monthly reviews.

f. The Directors, Organization Heads, and Commanders will:

(1) Designate (in writing) primary and alternate Web Content Managers (See Appendix B). Each organization may appoint no more than one "primary" and one "alternate" Web Content Manager. Other branch, section or staff content web managers may be appointed, but will report to their Web Content Manager. Give notification to the USFK Webmaster no less than 30 days in advance of a Web Content Manager's departure from the command, if an alternate Web Content Manager has not been appointed.
The appointment is intended as an additional duty but can be a primary duty at the discretion of the Director.

(2) Ensure that information within their purview, which is posted to the public access WWW information service, is accurate, timely and appropriate for public release. This includes establishing regular internal review procedures to ensure posted information continues to be appropriate, applicable and accurate.

(3) Comply with content guidelines provided by USFK PAO and technical guidelines by USFK J6, information security guidelines by USFK J2, and OPSEC guidance provided by J39.

g. The Web Content Managers will:

(1) Act as the liaison between the organization and the USFK Webmaster.

(2) Manage content of the organization webpage(s).

(3) Be responsible to submit information within their subject areas of expertise, and are responsible for the accuracy and release-ability of information within their purview.

(4) Coordinate information within the organization before submitting it for publishing and have a thorough understanding of public release policy and procedures, operations security, force protection, and classification of defense information under the purview of their Organization.

(5) Review the accuracy and appropriateness of the information to be released.

(6) Submit material to USFK PAO for review and approval, any new pages and changes to style or content of previously posted pages. Material for review should be submitted on compact discs (CDs) or digital video discs (DVDs). With prior USFK PAO approval organizations may submit small files via e-mail. Units with component and/or local PAO(s) should obtain servicing

PAO approval prior to forwarding material to USFK PAO. Submissions must include signed memorandum from Director, Special Staff/Organization Head or Commander, certifying prior approval and OPSEC and security review.

(7) Attend regularly scheduled meetings to discuss current status and future development of the public access WWW information service. These meetings will include, at a minimum, representatives from those organizations that actively contribute material and/or edit pages on the public accessible WWW information service.

(8) Comply with content guidelines provided by USFK PA and technical guidelines provided.

(a) Refer to Appendix B USFK Website Content Management Guidelines

(b) Refer to Appendix C for Content Evaluation Checklist for USFK Publicly Accessible Websites

(c) Refer to Appendix D to guard against possible breaches to operations security (OPSEC) by conducting a monthly check of the website. Maintain copies of each completed checklist (Appendix D) for a period of one year. If required, provide the USFK Webmaster with a list of information believed to compromise OPSEC and request the webmaster remove it from the website immediately.

(d) Conduct a monthly review of the website for information that has become outdated or no longer useful. Provide the USFK webmaster with a listing of material to be deleted or moved and retained for historical purposes, as appropriate.

h. The Component, installation, or local PAO(s) will:

(1) Review and approve subordinate unit web pages and material prior to posting to the USFK public access WWW information service to ensure the posted information is accurate, timely, appropriate for public release and IAW all applicable regulations and directives.

(2) Establish/implement a method for regular review to ensure posted information continues to be appropriate, applicable and accurate.

Chapter 2
Policy and Procedures

2-1. Policy

a. The mission/purpose of the USFK public access WWW information service is--
"To support the overall United States Forces Korea mission through the dissemination of publicly releasable information, for which Headquarters United States Forces Korea is directly responsible, materially satisfying the information needs or mission objectives of one or more intended audiences, while taking into account operational security, privacy considerations, and force protection."

b. The USFK Public Affairs Office (PAO) has overall content management control for the publicly accessible WWW service and related social networking, media sharing and online reference sites operated or maintained by USFK, and therefore has the authority to create, edit,

delete or move any information as deemed appropriate to meet ongoing Public Information (PI), Community Relations (COMREL) and Command Information (CI) objectives, requirements and initiatives. The USFK Webmaster will make every effort to coordinate with Organizations prior to taking action, unless the action is considered time sensitive and therefore will notify the Organization once the action is completed. Posting information to the WWW is equivalent to making a public release. All information must be properly cleared for public release. Proposals for new categories of information will also be forwarded to USFK PAO for review for approval to be posted on the WWW.

    c. The intended audiences of the USFK public access WWW information service are—

       (1) U.S. and international media;

       (2) U.S. and international institutions, organizations, and individuals;

       (3) USFK service members, civilians, contractors and family members;

       (4) Personnel with orders to report to USFK;

       (5) Reservists with mobilization assignments at USFK;

       (6)Other military commands and individuals;

    d. If the primary intended audience of an information product is the HQ USFK staff, another DOD organization, or a small subset of a larger audience, then the preferred means of dissemination is the HQ USFK or 8th Army Intranet, unclassified e-mail, or other means as practicable and/or appropriate. It is essential that the commander and other organizational heads review organizational information connectivity and content to ensure good OPSEC procedures are being applied within their organizations.

    e. Per DOD regulations, no information that is withholdable from the public pursuant to statute, or intended for restricted access or limited distribution, may be placed on a publicly accessible web information service. Nor should a public site have links to such information. This prohibition includes information that is classified, for official use only (FOUO), sensitive but unclassified, and privacy protected. Information cleared for public release under the Freedom of Information Act may be posted on publicly accessible web information services.

    f. Maintainers of publicly accessible web sites are specifically prohibited from posting the following type information:

       (1) Plans or lessons learned which would reveal sensitive military operations, exercises, or vulnerabilities.

       (2) Reference to any information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty regarding location is an element of the security of a military plan or program.

       (3) Any personal information in the following categories about U.S. citizens, DOD employees, and military personnel:

         (a) Social security account numbers.

(b) Dates of birth.

(c) Home addresses.

(d) Telephone numbers other than numbers of duty offices that are appropriately made available to the general public.

(4) Additionally, names, locations and any other identifying information about family members of DOD employees and military personnel should not be posted on publicly accessible WWW sites.

(5) The previous paragraphs should not be considered an all-inclusive listing of prohibited information. Part V, Examples and Best Practices, Section 2 of reference 3b(5), contains more detailed guidance for identifying information that is inappropriate for posting to publicly accessible DOD web sites. Commanders, reviewing personnel and web site developers and maintainers should make a concerted effort to ensure information of questionable public value that creates a potential security risk if made easily available to a worldwide audience is not posted to publicly accessible web sites.

g. Copyrighted material will be used only when allowed by prevailing copyright laws and may be used only if the materials relate to the command's mission. Consult with USFK JA prior to using any copyrighted material.

h. Under no circumstances will personal web server software, or a HQ USFK-assigned Internet Protocol (IP) address, be used to operate a separate, publicly accessible WWW service, without the express written approval of the Deputy Chief of Staff and the Command, Control and Communications Systems Organization (USFK J6) with the exception of social networking, media sharing and online reference sites setup and maintained by USFK PAO to meet ongoing PI, COMREL and CI mission objectives within the scope of the USFK PAO mission.

i. Posting of information to the public access WWW information service will be accomplished only by those personnel designated in writing by their Director, Commander or Special Staff Chief. The USFK Webmaster will only open a portal to post information upon confirmation of an approved Security and Policy review conducted by the USFK PAO.

j. The USFK public access WWW information service will present a neat and professional appearance, with a consistent design and user interface. New pages, and format or style changes to existing pages, will be staffed through the USFK PAO prior to posting.

k. Information posted on the public access WWW information service will be timely and accurate. Pages will be reviewed frequently and edited or deleted as necessary. Inaccurate information will be corrected promptly or deleted. Obsolete information will be deleted or moved and retained for historical purposes, as appropriate.

2-2. Consent to Monitoring
Use of government computer networks and systems is subject to monitoring. Activity on computer networks, government or otherwise, is not anonymous and does not provide any expectation of privacy.

2-3. Collection of Information

a. To better serve the command, in certain instances it is necessary and appropriate to collect information from visitors to websites. Office of Management and Budget (OMB) approves survey Forms and Information Collections from the public. Requests for identical information from ten or more members of the public must be approved by OMB, such as surveys using check box, radio button or text form fields.

b. Forms for general solicitations of comments that do not seek responses to standard questions, such as the common opinion-based feedback forms and e-mail links, do not require OMB clearance.

c. According to the type of information being collected, the approval process by OMB may take more than six months. It is the responsibility of the organization or staff to request OMB approval for online collections of information. Please contact the USFK Webmaster during the early planning stages to ensure all web issues are addressed.

2-4. Policy Violations

a. A service member or government employee has a duty to protect and conserve government property. This duty requires that the service member or government employee not use, or allow the use of, government property for other than authorized purposes. Misuse of government property could constitute a violation of the standards and rules of conduct prescribed by DOD 5500.7-R (Joint Ethics Regulation (JER)), with change 6. Violations of DOD 5500.7-R by service members may result in prosecution under the Uniform Code of Military Justice (UCMJ), as well as adverse administrative action or other adverse action authorized by the United States Code or Federal Regulations. Violations of DOD 5500.7-R by government employees may result in the full range of statutory and regulatory sanctions, to include adverse administrative action or other adverse action authorized by United States Code or Federal Regulations.

b. Failure to comply with provisions of this regulation may also result in revocation of computer system accounts and/or loss of access to all USFK automated information systems, and could lead to punishment under the UCMJ, termination of employment, and criminal prosecution.

Appendix A
References

Section I. Required Publications

DOD 5500.7-R, Joint Ethics Regulation (JER), 1993, Certified Current as of December 3, 2008. Cited in paragraph 2-4.

United States Code or Federal Regulations. Cited in paragraph 2-3.

Section II. Related Publications

Air Force Instruction 33-129, Web Management and Internet Use

Army Regulation 25-1, Army Knowledge Management and Information Technology

SECNAV Instruction 5720.47B, Department of the Navy Policy for Content of Publicly Accessible World Wide Web Sites

DOD policy memorandum, Establishing and Maintaining a Publicly Accessible DOD Web Information Service, 18 July 1997 (Updated January 9, 1998).

Deputy Secretary of Defense Policy Memorandum, Web Site Administration, 7 December 1998 (Updated January 11, 2002).

Deputy Secretary of Defense Policy Memorandum, Government Information Locator Service (GILS), 2 September 1995.

Office of Management and Budget (OMB) Bulletin 95-01, Establishment of Government Information Locator Service, December 7, 1994.

DODD 5230.9, Clearance of DOD Information for Public Release

DOD 5400.7-R, DOD Freedom of Information Act Program, September 29, 1998, with change 1 dated April 11, 2006.

DODI 5230.29, Security and Policy Review of DOD Information for Public Release

DODD 5240.1, DOD Intelligence Activities

DOD 8910.1-M, DOD Procedures for Management of Information Requirements

Public Law, The Computer Security Act of 1987.

Children's Online Privacy Protection Act (COPPA), Public Law 105-277, 15 US Code §§ 6501-6506.

USCINCPAC Message 1220352 OCT 98, Subj: NIPRNET OPSEC Guidance.

USCINCPAC Message 1404252 NOV 98, Subj: Combatant Web Site Review.

USCINCPAC Message 2601 152 MAR 98, Subj: NIPRNET Theater OPSEC Guidance

Army Regulation 530-1, Operations Security, 19 April 2007

CFC/USFK Operations Publication 3-4.9, OPSEC, 1 January 2007

Appendix B
USFK Website Content Management Guidelines

B-1. Summary
Publishing information that promotes command objectives, while taking into consideration security, privacy and force protection issues, is a critical aspect of a Web Content Manager's duties. It is better to err on the safe side when considering these matters and withhold publication of questionable material until further review.

B-2. Action

a. In the event that a Web Content Manager has a question about whether or not specific material might adversely affect the command, consult your operations security (OPSEC) manager.

b. Web Content Managers will decline to publish information on the USFK public website in the following specific instances:

(1) **Operations, Plans and Training.** Information that provides extensive details of military plans, operations, exercises or lessons learned that would reveal vulnerabilities or compromise future planning; details of mission-specific training; any information that would reveal sensitive movements of military assets or the location of units or personnel where uncertainty regarding location is an element of the security of a military plan or program; detailed exercise, deployment or training schedules; inspection results, findings and deficiencies; unit vulnerabilities or weaknesses; advanced planning of unit relocation or deployment; and listings of classified topics or detailed discussion of topics that in combination might compromise mission objectives or classified information. (Example: A detailed syllabus on topics concerning anti-terrorism measures to be presented as part of a class on physical security.)

(2) **Personal Information.** Social Security numbers; dates of birth; home addresses; home telephone numbers and home e-mail addresses; names, location or any other identifying information about family members of military personnel or DOD employees. This is particularly important when publishing biographies.

(3) **Technological Data.** Weapons schematics, weapon system vulnerabilities, electronic wire diagrams, and frequency spectrum data.

(4) **Administrative.** Personal travel information, attendance at conferences, and commercial support contracts. Non-disclosure of travel information and attendance at conferences is particularly important when concerning senior government officials and general or senior officers.

(5) **Communications.** RF emissions and associated documentation; changes in activity or communications patterns; organization, architecture, and usage patterns of computer networks and systems (both classified and unclassified); and availability of secure communications.

(6) **Logistics/Maintenance.** Supply and equipment orders and deliveries; transportation plans; maintenance and logistics requirements; and receipt or installation of special equipment.

(7) **Maps/Photos.** Aerial view photos or maps of installations and facilities that may be informative or sensitive in nature (e.g. aerial view of Yongsan Army Garrison).

c. Use Appendix D, USFK Operations Security (OPSEC) Checklist, as a day-to-day guide for web content management of USFK publicly accessible websites.

B-3. <u>Conclusion</u>
Web Content Managers should treat the unclassified USFK website as they would any other external communications vehicle, ensuring material published does not compromise operational security, privacy considerations, or force protection. Security of information on a publicly accessible website, therefore, must be viewed in the context of USFK's overall operational security and force protection posture.

Appendix C
Content Evaluation Checklist for USFK Publicly Accessible Websites

Content Evaluation Checklist For USFK Publicly Accessible Websites:			
Name:	Date/Time of Evaluation:		
Directorate Reviewed:	Primary IP Address/URL:		
Issue/Concern:		Yes	No
1. Site does not require CAC enabled sign-in or other password. 2. Site does not contain any classifications or markings such as "Approved for Public Release." Site only contains unclassified information. 3. Information on the site is up to date. Outdated information is removed. 4. Web Content Manager's contact information is available including the organization, a phone number, and organizational email address on each significant page. 5. Site provides a feedback or request for further information mechanism (email or form). Generic organizational email addresses are used. 6. No "under construction" notices posted. Only complete, functional pages are authorized. 7. Appearance of web is professional. Subordinate pages are recognizable as part of the overall site. 8. Web pages load quickly and are not hampered by large graphics. 9. Graphics, animations and sound files are limited and purposeful and do not detract from the overall quality of the website. 10. Site contains links to subordinate sites. 11. Site contains links to higher headquarters sites. 12. There are no inactive or broken links. 13. Navigation system is simple, intuitive and consistent throughout the site. 14. Web-based message boards, threaded chat rooms and guest books are not used. 15. Site does not contain classified records. 16. Site does not contain records or information on internal personnel rules and procedures. 17. Site does not contain confidential commercial or proprietary information. 18. Site does not contain information exempt by a specific statute (i.e., maps, charts, and geodetic data; names and other personally identifying information for personnel; contractor proposals; etc.). 19. Site does not contain inter-and intra-agency records (i.e., drafts, pre-decisional data, attorney work products, etc.). 20. Site does not contain investigative records. 21. Site does not contain financial records. 22. Site does not contain geological/geophysical information. 23. Site does not contain commercial advertising or product endorsements.			

24. Site does not contain references to movement of military assets or personnel; the location of units, installations, or personnel where uncertainty is an element of security of a military plan, program or personnel; or military plans, exercises, assets or vulnerabilities.

25. Site does not contain personally identifying information on DOD personnel, to include names, ranks, email addresses, phone numbers, SSNs, and birth dates. There are no lists of names on rosters, directories, telephone directories, or organizational charts. Exceptions are Public Affairs products.

26. The only biographies available on the site or linked to by the site are those of key leaders, or personnel who by nature of their position and duties frequently interact with the public. Key leaders are identified as brigade/wing commanders or their equivalent and above. Biographies must not reveal names, addresses or other identifying material of family members of USFK employees or members.

27. Copyrighted material is only used with written permission from the owner. This includes, but is not limited to, computer software, sequences of code and instructions.

28. There are no trademarks or copyrighted logos posted.

29. Site does not link to restricted sites without approved security measures in place. (Secured or CAC required sites)

30. Errors generated by public attempts to access restricted pages do not include language such as "access denied" or "forbidden." Redirection back to the public site is automatic and transparent.

31. Site does not link to inappropriate or offensive sites.

32. External links consider needs of personnel and their families, mission-related needs, public communication and community relations objectives.

33. External links support the organization's mission.

34. External links do not endorse products or give preferential treatment.

35. External links have not been placed in exchange for payment nor do they contain graphics or logos depicting the company or products.

36. Site does not encourage users to choose a specific browser.

37. Disclaimer found in AFI 35-101, 18.6.2.10, is posted when linking to external sites.

38. Site frames are not continued outside the purview of the unit's site and authority.

39. Links to authorized activities (e.g. AAFES) that contain advertising give the appropriate disclaimer. See AFI 35-101, 18.6.2.10.

40. Links to non-government sites contain the appropriate disclaimer. See AFI 33-129, 8.2.1.3.

41. Site does not contain persistent electronic tracing devices, sometimes referred to as cookies.

42. Site gives privacy advisories whenever personally identifying information is solicited from an individual and the information is not maintained in a system of records. The advisories tell the individual why the information is needed, how it will be used, and how it will be stored and protected.

43. Site gives Privacy Act Statement whenever soliciting information from an individual that is part of a Privacy Act system of records. The Privacy Act Statement tells the individual the authority, purpose, routine use, and whether disclosure is voluntary or mandatory.

44. Site contains the security and privacy notice found in AFI 33-129, 13.1.

Appendix D
Operations Security Checklist for USFK Publicly Accessible Website

Operations Security (OPSEC) Checklist For USFK Publicly Accessible Websites:				
Name:	Date/Time of Review:			
Directorate Reviewed:	Primary IP Address/URL:			
Issue/Concern:		Yes	No	Notes/ Comments:
Management Controls (*Note 1*): 1. Does the Website (WS) contain a clearly defined purpose statement that supports the USFK mission? 2. Are users of this WS provided with privacy and security notices prominently displayed or announced on at least the first page of the site? 3. If applicable, does this WS contain a "disclaimer for external links" notice for any site outside the DOD or federal government? **Operations, Plans and Training (*Note 2*):** 1. Does the WS contain information that provides extensive details of military plans, operations, exercises or lessons learned that would reveal vulnerabilities or compromise future planning? 2. Does the WS contain details of mission-specific training? 3. Does the WS contain any information that would reveal sensitive movements of military assets or the location of units or personnel where uncertainty regarding location is an element of the security of a military plan or program? 4. Does the WS contain detailed exercise, deployment or training schedules? 5. Does the WS contain inspection results, findings or deficiencies? 6. Does the WS contain unit vulnerabilities or weaknesses? 7. Does the WS contain information on advanced planning of unit relocation or deployment?				

Personal Information:

Does the WS contain personal information in the following categories about U.S. Citizens, DOD employees and military personnel:

    a. Social Security Account Numbers?
    b. Dates of Birth?
    c. Home Addresses?
    d. Home telephone numbers or home email addresses?
    e. Names, location or any other identifying information about family members?

Technological Data (*Note 3*):

Does the WS contain technical data such as:

    a. Weapon schematics?
    b. Weapon System Vulnerabilities?
    c. Electronic Wire Diagrams?
    d. Frequency Spectrum Data?

Administrative:

Does the WS contain relevant information in the following categories that might reveal an organization's plans and intentions?

    a. Personnel Travel (personal or official business).
    b. Attendance at planning conferences.
    c. Commercial support contracts.

Communications:

Does the WS contain information on any of the following?

    a. RF emissions and associated documentation.
    b. Changes in activity or communications patterns.
    c. Organization, architecture, or usage patterns of computer networks and systems. (either classified or unclassified)
    d. Availability of secure communications.

Logistics/Maintenance:

Does the WS contain information on any of the following?

    a. Supply and equipment orders/deliveries.
    b. Transportation plans.
    c. Maintenance or logistics requirements.
    d. Receipt or installation or special equipment.

Maps/Photos:

Does the WS contain information on any of the following?

    a. Aerial view photos or maps of installations or facilities that may be informative or sensitive in nature.
    b. Detailed routes local military personnel may often travel.
    c. Photos of visible force protection measures.

Key Word Search (*Note 4*):

Using the following "key words" conduct a search using the search tool. As a result of this search conduct a random screen of any documents found:

    a. Deployment Schedules
    b. Exercise Plans
    c. Contingency Plans
    d. Training Schedules
    e. Inspection results, findings, deficiencies
    f. Biographies
    g. Family Support Activities
    h. Phone Directories, Lists

Does the WS contain any classified, unclassified but sensitive, or for official use only data?

YES   NO

-NOTES PAGE-

No information that is withholdable from the public pursuant to statute, or intended for restricted access or limited distribution, may be placed on a publicly accessible web information service; nor should a public site have links to such information. This prohibition includes information that is CLASSIFIED, UNCLASSIFIED but SENSITIVE, FOR OFFICIAL USE ONLY (FOUO), and privacy protected. Posting information to the WWW is equivalent to making a public release, and per DOD Directive 5230.9, all information must be properly cleared.

Note 1: Management Controls are contained in the policy published by the Office of the Secretary of Defense, titled: Establishing and Maintaining A Publicly Accessible Department of Defense Web Information Service, 9 January 1998.

Note 2: These elements were pulled directly from the DEPSECDEF memo, Information Vulnerability and the World Wide Web, dated, 24 Sept 98.

Note 3: Technical data creates a unique challenge to the OPSEC posture of an organization and to National Security as a whole. Certain technical data, when compiled with other unclassified information, may reveal an additional association or relationship that meets the standards for classification under Section 1.8 (e) E.O. 12958.

Note 4: There are many other "key words" possible to denote the wide range of USFK's military operations and activities. Web Content Managers are encouraged to search using other key words as may be applicable based on their Organization's portion of the USFK mission. Within the context of information assurance, the World Wide Web should not be treated any differently than any other potential vulnerability. Security of information on publicly accessible websites must be viewed in the context of USFK's overall OPSEC posture.

Glossary

Section I
Acronyms and Abbreviations

8th Army	Eighth United States Army
CAC	Common Access Card
CI	Command Information
COMREL	Community Relations
DOD	Department of Defense
EMO	Electronic Media Only
FOUO	For Official Use Only
GILS	Government Information Locator Service
HQ	Headquarters
IAW	in accordance with
IP	Internet Protocol
JER	Joint Ethics Regulation
OMB	Office of Management and Budget
OPSEC	Operations Security
PA - PAO(s)	Public Affairs - Public Affairs Office(s)
PI	Public Information
PII	Personally Identifiable Information
UCMJ	Uniform Code of Military Justice
U.S.	United States (of America)
USFK	United States Forces Korea
WS	Website
WWW	World Wide Web