

14 September 2004

Information Management: Automation

Web Site Administration

---

For the CG, USAREUR/7A:

E. PEARSON  
*Colonel, GS*  
*Deputy Chief of Staff*

Official:



GARY C. MILLER  
*Regional Chief Information*  
*Officer - Europe*

---

**Summary.** This regulation establishes policy and procedures for use of Internet, intranet, and extranet Web sites.

**Applicability.** This regulation applies to Army in Europe personnel and organizations that use information systems.

**Supplementation.** Organizations will not supplement this regulation without USAREUR G6 (AEAİM-A-P) approval.

**Forms.** AE and higher level forms are available through the Army in Europe Publishing System (AEPUBS).

**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 Management System Web site at <https://www.arims.army.mil>.

**Suggested Improvements.** The proponent of this regulation is the USAREUR G6 (AEAİM-A-P, DSN 370-7395). Users may suggest improvements to this regulation by sending DA Form 2028 to the USAREUR G6 (AEAİM-A-P), Unit 29351, APO AE 09014-9351.

**Distribution.** B (AEPUBS).

---

CONTENTS

SECTION I  
INTRODUCTION

1. Purpose
2. References
3. Explanation of Abbreviations and Terms
4. Responsibilities
5. General
6. Training

7. Web Site Reviews and Inspections
8. Metadata Tagging Requirements
9. Section 508 Compliance
10. Data Backup
11. Server Authorization
12. Access Control
13. Links
14. Records Management
15. Standard Army Management Information System (STAMIS) Web Sites
16. Deployed Organizations

## **SECTION II INTERNET WEB SITES**

17. Definition
18. Public Affairs Approval
19. Approval Process

## **SECTION III EXTRANET WEB SITES**

20. Definition
21. AKO
22. Access-Control Requirements
23. Approval Process
24. Encryption Standard

## **SECTION IV INTRANET WEB SITES**

25. Definition
26. Access-Control Requirements
27. Approval Process
28. Encryption Standard

### **Appendixes**

- A. References
- B. Public Affairs Content Approval Checklist
- C. Public Affairs Web Site Review Checklist
- D. OPSEC Web Site Review Checklist
- E. Information Infrastructure Assistance Team Inspection Checklist
- F. AE Metadata Tag Standard

### **Glossary**

---

## **SECTION I INTRODUCTION**

### **1. PURPOSE**

This regulation prescribes AE-unique requirements for operating unclassified Web servers (Internet, intranet, and extranet) to ensure information is accessible to authorized audiences at the time and place necessary to help them accomplish the mission, implement strong information assurance (IA) measures, and ensure force protection.

### **2. REFERENCES**

Appendix A lists references.

### **3. EXPLANATION OF ABBREVIATIONS AND TERMS**

The glossary explains abbreviations and terms.

#### 4. RESPONSIBILITIES

**a. USAREUR G6.** The USAREUR G6 will establish policy to install, operate, and maintain (IOM) Web servers and Web sites for AE organizations.

**b. Chief, Public Affairs (CPA), USAREUR.** The CPA has responsibility for the approval of all content on all publicly accessible USAREUR Internet Web sites. The IMA-E Public Affairs Office (PAO) will perform this function for IMA-E organizations. The CPA and IMA-E PAO will—

(1) Develop and maintain a set of common templates for use by AE organizations in posting content on their publicly accessible Internet Web site. IMA-E organizations will post public content on the IMA public server. (Section II has more information on public servers.)

(2) Provide checklists for unit PAOs to use when evaluating content for publication, review, or inspection.

**c. Information Technology Support Activity (ITSA).** ITSA will provide—

(1) Server manager functions for Web server hardware and system administration.

(2) Technical support for Army in Europe organizations that publish publicly accessible information on the USAREUR Internet site and for HQ USAREUR/7A staff office private sites under ITSA management.

**NOTE:** The USAREUR G6 will have operational control of ITSA Web services.

**d. Unit Data Owner (Originator/Proponent).** The unit data owner is the person who will provide original content or information to a Web site. This person is responsible for determining and marking the sensitivity of the document, determining the appropriate audience for the information, and getting approval from the local PAO, operations security (OPSEC) office, and commander (or designated representative) before requesting publication of information. The data owner will participate in the internal quarterly review and periodically review content to ensure it is current and properly protected.

**e. Unit PAO Officer.** The unit PAO officer will be designated by the commander on duty appointment orders. Unit PAO officers will review information for release to the unit's publicly accessible Internet Web site and will coordinate with the CPA or IMA-E PAO when necessary. No information will be posted to a publicly accessible Web site without a review and recommendation from the unit PAO officer and approval from the unit commander (or civilian equivalent) or content manager. The unit PAO officer will use the checklist in appendix B to evaluate information and provide a recommendation to the commander or content manager. The unit PAO officer will use the checklist in appendix C to conduct the unit's internal quarterly review.

**f. Unit OPSEC Officer.** The unit OPSEC officer will provide an OPSEC review of content at the unit level during the Web content-approval process (app D). Information will not be posted on any unit Web site (Internet, intranet, or extranet) without this OPSEC review and approval from the approving authority. The OPSEC officer will send requests for additional OPSEC support through the parent headquarters OPSEC officer to the USAREUR OPSEC Program Manager (for OPSEC training), the 1st Information Operations Command (1st IOC) (for external support), or other appropriate agencies. The unit OPSEC officer will conduct periodic Web reviews of unit Web pages with unit PAO officers, Web masters or Web authors, content managers, and data owners.

**g. Unit Content Manager.** Content managers are normally assigned at battalion level and higher (and at equivalent agencies that have an internal staff). The unit content manager will work closely with the unit records manager to manage information created by an organization to ensure it is authentic, current, accessible to the authorized audience, preserved, and protected. Content managers will coordinate with unit data owners, commanders, unit Web masters, and Web authors to provide information to the intended audience. Content managers will coordinate quarterly internal reviews of all Web site information.

**h. Unit Web Master.** The unit Web master is the individual or group who administers the Web site hardware and software for AE units that are authorized Web servers (where server consolidation has not already occurred). Web masters will—

(1) Design Web site layout.

- (2) Provide necessary encryption and access controls.
- (3) Post information in compliance with the data owner, commander or content manager, and governing policy.
- (4) Coordinate internal reviews of Web site information.
- (5) Have technical control over updating the site's content.
- (6) Ensure the site conforms to Federal, DOD, and Army policy and conventions.

**NOTE:** AE units that are authorized to have Web servers will not operate them without a qualified Web master.

**i. Unit Web Author.** Where server consolidation has occurred, the unit Web author is the person that coordinates with the server manager to post content to unit Web sites. Unit Web authors—

- (1) Design Web site layout.
- (2) Provide appropriate encryption and access controls.
- (3) Coordinate with the Web master to post information in compliance with the data owner, commander or content manager, and governing policy and regulations.

**j. Unit Records Manager or Records Coordinator.** The unit records manager or records coordinator is the person appointed to ensure record information in the organization is identified as such and that appropriate maintenance and protection measures are used. Records managers and records coordinators provide guidance, advice, and assistance to data owners, content managers, and commanders.

**k. Unit Commander or Equivalent Civilian Leader.** The unit commander or equivalent civilian leader—

- (1) Will determine the type of Web sites (Internet, extranet, intranet) necessary to publish information to support the mission.
- (2) Is the final approval authority for information published by the organization.
- (3) May delegate approval authority to publish information to the unit content manager.

**l. Server Manager.** Where server consolidation has occurred, the server manager (for example, ITSA) IOMs the Web server hardware and software that units use to establish their Web presence.

## 5. GENERAL

a. Primary consideration must be given to IA and OPSEC requirements before posting any information online. Posted information must be correctly identified, marked, categorized, and placed on the correct network and Web site with the correct access controls required in this regulation.

b. Personnel will follow DOD and DA guidance, policy, and regulations on Web site operations, OPSEC, and IA. Use only the LandWarNet (Class) system to develop, review, approve, and post classified information. While it is permissible to load unclassified information into a classified system when the mission dictates, at no time will classified information be entered into a LandWarNet (Unclas) system.

## 6. TRAINING

a. Web master and Web author training and certification is required before these personnel may operate any Web site in the Army in Europe. Units must identify, train, and certify their Web personnel as follows:

- (1) Web masters and Web authors must be designated on official duty appointment orders by the unit commander. A current, signed copy of these appointment orders must be kept in unit records and provided to the USAREUR training organization when attending certification training courses.

(2) Web masters and Web authors must complete the DA Web Masters Training Module at <https://iatraining.us.army.mil>. The individual will keep an official record of the certificate of completion of training in official unit records. This training is a prerequisite to the AE Web Master Security Course in (3) below.

(3) Web masters and Web authors must attend and successfully complete the AE Web Master Security Course and test before being designated as a primary Web master or Web author for their unit. Attendance at this course may be requested through <https://www.uatp.hqusareur.army.mil/>. Allocation of training seats will be given to primary Web masters and Web authors first, alternate Web masters or Web authors second, personnel in content manager positions third, and all others as available. Personnel must provide a signed copy of appointment orders ((1) above) as part of the request to attend the course. Units that do not have a qualified Web master will not operate Web server equipment. This restriction will become effective 1 January 2005 to provide time for units to get personnel trained and qualified. The certificate of completion must be kept in official unit records.

(4) Web masters must have a DA-level II information assurance and computer network defense (IACND) certification to IOM Web servers.

b. Content managers must be designated on official duty appointment orders by the unit commander. These orders must be kept in unit records. Content managers must attend and successfully complete the AE Content Manager Training Course and test before being designated as the content manager for their unit. Attendance at this course may be requested at <https://www.uatp.hqusareur.army.mil/>. Training seats will be allocated to primary content managers first, primary Web masters or Web authors second, alternate content managers third, and all others as training seats are available. Personnel must provide a signed copy of their duty appointment orders as part of the request to attend the course. The certificate of completion must be kept in official unit records.

c. Server managers must have a DA-level II IACND certification to IOM Web servers.

## 7. WEB SITE REVIEWS AND INSPECTIONS

**a. Internal.** The unit content manager will coordinate a formal quarterly review of each unit Web site with all data owners who have published information on the site. The review will validate the sites to ensure the content is current, protected as required, or removed. The Web master or Web author should remove content if data owners fail to conduct their quarterly review. The results of the review are subject to inspection and must be documented and maintained in unit records according to AR 25-400-2.

**b. External.** Inspections must be conducted to ensure units comply with this regulation. Units that score less than 70 percent on an inspection or that have major public affairs, OPSEC, or IA shortcomings must terminate Web operations until the deficiencies have been corrected.

(1) The Information Infrastructure Assistance Team (I2AT) (from the Office of the G6, HQ USAREUR/7A) will conduct an annual inspection of each USAREUR major subordinate command (MSC) and area support group (ASG) to ensure they are complying with this regulation. The team will use the checklist in appendix E to conduct these inspections.

(2) The Command Inspection Program for each unit will include inspection of subordinate units' Web programs using the checklist in appendix E. The unit records manager will review records related to this policy to ensure the unit is complying.

(3) The CPA and IMA-E PAO will conduct a quarterly review of subordinate organizations' publicly accessible Web sites using the checklist in appendix B. Any site that is not in compliance must be taken offline (out of service) until corrections are made and reported to the CPA or IMA-E PAO (as appropriate).

(4) Web sites must be included in normal records-management inspections conducted every 2 years in the European theater. This will ensure record information is identified and maintained according to Army records management policy and procedures.

**c. Ongoing Review.** The USAREUR G3, USAREUR G6 (AEAIM-IAPM), and Regional Computer Emergency Response Team (RCERT) will monitor AE Web sites and may direct AE units to terminate Web operations (or designated parts of it) if they are violating OPSEC, IA, or network requirements.

(1) If an OPSEC, IA, or network vulnerability is identified, the identified page, link, or information must be removed from the Web site immediately and stay off until action is taken to correct it according to DOD and AE directives.

(2) As soon as a problem is identified, the Web master or author responsible for the Web site or page will be notified. Notification will include instructions to take the page or link offline, the specific vulnerability or deficiencies identified, and recommended remedial action.

(3) Unit POCs who have content and review responsibilities in paragraph 4 will convene an informal review board to investigate the problem and take remedial action as soon as possible.

(4) After taking remedial action, unit POCs will submit the corrected page to the office that required the removal action for verification and request authorization to place the content online.

**d. Ad Hoc Review.** If an individual believes a Web site may have an OPSEC or IA violation, that individual should contact the Web master or Web author for the site. The Web master or Web author will investigate to determine whether a violation has occurred and take action with the unit PAO, OPSEC office, content manager, and commander to address the concern. The Web master or Web author will then send findings from the investigation and actions taken to the individual who raised the concern. The concern may be raised to the offices in subparagraph c above for further action if necessary.

## **8. METADATA TAGGING REQUIREMENTS**

a. Metadata enables sophisticated indexing, identification, and searching of information. The proponent of the information is responsible for developing the metadata used to identify the information (such as Web pages and files available on a Web site). The Web master or Web author will code the metadata into the HTML header. Units must immediately begin using metadata tagging on all new information and pages. Units also must implement a program to add metadata tags to old pages and information by 1 August 2005.

b. The metadata tags in appendix F must be used for all Web pages and files created by Web masters and Web authors.

c. When an application does not automatically create metadata during the preparation of the document, data owners will complete and submit the metadata template in appendix F when submitting information for publishing on a Web site. Web masters and Web authors will use the template to develop the metadata code for the information.

## **9. SECTION 508 COMPLIANCE**

All AE Web sites (intranet, extranet, and Internet) must comply with Conformance Level A requirements (all priority 1 checkpoints are met) of the Rehabilitation Act, Section 508 (<http://www.section508.gov/> or <http://www.w3.org/TR/WAI-WEBCONTENT/checkpoint-list.html>). Units must ensure all new Web pages comply with Section 508 of the Rehabilitation Act. Units also must implement a workable program to bring old pages and information into compliance by 1 August 2005. Priority of Section 508 work will be given to the unit's public site and then to private sites. Units will show Conformance Level A compliance by affixing the accessibility icon (found as Level A icon at <http://www.w3.org/WAI/WCAG1-Conformance>) at the bottom of the front page to their sites. The icon will be "hot linked" to additional unit information about their compliance with Section 508. This includes contact information (e-mail address and telephone number for the unit content manager).

## **10. DATA BACKUP**

To ensure integrity and availability of original information created by an organization, the content manager and Web master or server manager will ensure all information posted to AE Web sites is backed up so it can be fully restored in case of hardware failure or other unplanned or catastrophic event that would destroy the information on the production system. The preferred method of data backup will be to back up information on a separate storage system not located in the same facility as the Web server. In those units where a local tape drive or backup system is used, the unit must ensure that the back-up tapes are stored and secured in a separate facility from the Web servers. The backup interval must be according to the system security authorization agreement (SSAA) established when the system was approved for operation. A full backup must be completed each week with incremental backups each day. The Web master (or Web author with the server manager) will keep a current copy of the full backup in a separate location approved to store the highest security classification level of information that is included in the backup.

## **11. SERVER AUTHORIZATION**

When a commander determines there is a need for a new requirement for sharing information through Web services, the unit must request resource support based on the following:

a. In the consolidated server environment where all servers have been consolidated in a network service center (NSC) or other designated consolidated facility (such as ITSA) and to facilitate the Army Knowledge Management (AKM) server consolidation requirements, AE NSCs and other designated consolidation facilities will IOM Web server hardware and software in coordination with their supported units.

(1) If a commander (or civilian equivalent) determines a need to establish an intranet or extranet, he or she will request support from the NSC or other consolidation facility.

(2) If the NSC or other consolidation facility has server capacity to support the requirement, it will enter into a service level agreement with the commander to establish the parameters to IOM the server.

(3) If current capacity does not exist or is insufficient, the commander may procure the necessary hardware and software to establish the Web servers in the NSC or other consolidation facility with a service level agreement.

(4) Server systems that are new requirements and not already covered by a higher-level certificate of networkiness must be certified as required at <https://www.dcsim.hqusareur.army.mil/cto/>.

b. In the nonconsolidated environment (where full USAREUR G6 (AEAİM-TFE) server consolidation initiative has not yet occurred or is not feasible), Web server hardware and software is authorized at MSC level and higher. MSCs must meet all requirements of this regulation to operate these systems. Server systems that are new requirements and not already covered by a higher-level certificate of networkiness must complete the certification process as required at <https://www.dcsim.hqusareur.army.mil/cto/>.

c. CPA with ITSA will establish the USAREUR Internet (public) Web site and provide authoring capabilities for all USAREUR organizations that have a requirement to release publicly accessible information. All IMA-E organizations will host their public access Web sites on the IMA single public server. Units that have Web servers must have a qualified Web master assigned on appointment orders to IOM the server.

## **12. ACCESS CONTROL**

The data owner (proponent of the information) will determine the sensitivity of the information and the authorized audience. The data owner will coordinate the required access-control requirements with the Web author or Web master, the content manager, and the server manager. This coordination must ensure appropriate access controls are set on each unique information document posted and that each document is placed on the Web site best suited for the intended audience. Additional access-control requirements are in sections III and IV.

## **13. LINKS**

a. Hyperlinks are an excellent way to allow users to share information. Generally, links from publicly accessible sites to private sites (intranet or extranet) will not be used. If a public site provides a link to a private site to support the organization's mission, it must—

(1) Have a notice to advise that the link is protected.

(2) Provide contact information.

b. Web masters, Web authors, and unit data owners will not republish or post information that is already accessible on the originating organization's Web site. The Web master and Web author may provide a link to the information on the site that hosts the information.

## **14. RECORDS MANAGEMENT**

Information posted on Web sites that provides evidence of the organization, functions, policy, decisions, procedures, operations, or other activities of the U.S. Government must be identified and handled as record information under AR 25-400-2. The organization's records manager or records coordinator will provide assistance in applying retention standards and handling procedures to the information.

## **15. STANDARD ARMY MANAGEMENT INFORMATION SYSTEM (STAMIS) WEB SITES**

Units that operate STAMIS or other special business-process servers that provide a Web-based front-end as part of their business process must ensure these systems fully comply with this regulation where it is technically possible and within the authorization (responsibility) of the unit to make system changes. DA STAMIS Web sites are exempt from the exception process in paragraph 21a but must have an active link from the unit's Army Knowledge Online (AKO) portal if the system is to be shared with the unit's extranet audience.

## **16. DEPLOYED ORGANIZATIONS**

Units that will deploy to conduct operations away from their home station for more than 30 days must plan for the continued use, operation, and maintenance of their Web sites. Units will do one of the following in this situation:

a. Cease all Web site operations and temporarily remove the servers from the network until the unit returns to the home station. When this option is chosen, the unit will—

(1) In consolidated environments, advise the server manager, the next higher headquarters, and the USAREUR G6 of its intention to terminate all Web site operations on a specified date and provide the estimated date that the server will be returned to service. The unit will provide the uniform resource locator (URL), Internet protocol (IP) address, and the type of sites involved (Internet, intranet, extranet). The unit will create a full backup of the Web sites and store this information so that it is fully identified, safeguarded, and recoverable. The unit will request that the server manager fully disable access to its Web sites.

(2) In the nonconsolidated environment, complete the actions in (1) above and will disable the Web servers by removing the network cable, fully powering down the system, and marking the system to fully identify it and its purpose and the expected date to reestablish the site. The system will not be used for other purposes during the period of deployment.

**NOTE:** When the unit returns to its home station, the unit content manager will conduct a full internal review before placing the sites back into production if the unit was deployed for more than 90 days.

b. Maintain limited or full Web site operations during the deployment. Web sites that will be terminated during the period of deployment will follow the policy in subparagraph a above. Unit Web sites that continue to be in operation must meet all requirements of this regulation. Unit Web sites that do not meet all requirements of this regulation will have their servers blocked at the network or server manager level until they are brought into full compliance.

## **SECTION II INTERNET WEB SITES**

### **17. DEFINITION**

An "Internet Web site" includes information technology (IT) hardware and Web server software that provides access to publicly releasable information through the World Wide Web. Information placed on an Internet Web site can normally be accessed by any computer system connected to the Internet. Only the CPA and ITSA may operate Internet (public) Web server hardware for USAREUR units. IMA-E organizations will use the IMA public server according to the IMA Web Site Administrative SOP.

### **18. PUBLIC AFFAIRS APPROVAL**

Any unit commander who decides to establish a new Internet site on the USAREUR public Web server must have the site content reviewed by the CPA before it is activated and made available to the public. The CPA will provide the public affairs seal, which must be included on the front page of the site. New IMA-E organizational Web sites will be submitted to the IMA-E PAO for approval and will affix the IMA seal to the site after approval. IMA-E organizations will use the IMA public server according to the IMA Web Site Administrative SOP.

### **19. APPROVAL PROCESS**

a. Before data owners request approval to publish any document, they will—

(1) Develop the metadata for the data to be posted (para 8).

(2) Determine the authorized audience. This will determine which offices must review the content and help the content manager and Web author or Web master determine which Web site (Internet, extranet, intranet) the information should be posted on and what access controls must be implemented.

b. After completing the items in subparagraph a above, data owners will—

- (1) Get approval from the supporting OPSEC office for information to be published on their public site.
- (2) Get approval from the responsible PAO for information to be published on their publicly accessible Web site.

(3) After receiving OPSEC and PAO approval, get commander or content manager final approval to publish the information on the Web site. The content manager will coordinate with the commander as required and, if the information is approved for publication, will provide necessary publishing instructions to the Web master or Web author.

## **SECTION III EXTRANET WEB SITES**

### **20. DEFINITION**

An “extranet Web site” includes IT hardware and Web server software that provides protected, limited, or restricted access to information that will be shared outside of the organization but not with the public at large. Sensitive and For Official Use Only (FOUO) information (AR 25-11 and AR 25-55) must have “need-to-know” (or other) criteria applied to determine if access should be limited to a specific group or organization within the broader audience.

### **21. AKO**

The AKO Web site will be the first tool (Web-server system) for commanders to use when they determine a need exists for an extranet Web presence. The unit will request a portal page and knowledge community center (KCC) from the USAREUR G6 (AEAIM-AS). The request must include a copy of the unit Web master or Web author duty appointment orders. The USAREUR G6 (AEAIM-AS) will create the basic portal and KCC and assign administrator privileges to the unit Web master or Web author and to the content manager.

a. Requests for exception to using the AKO portal for a unit’s extranet Web site must—

- (1) Explain what the system will do.
- (2) Explain why AKO cannot meet the requirement.
- (3) Document the resources (personnel, funds, and equipment) that will be required to IOM the system for its life-cycle.

(4) Be sent by e-mail to [aeaim-xo@hq.hqusareur.army.mil](mailto:aeaim-xo@hq.hqusareur.army.mil) or to the USAREUR G6 (AEAIM-X), Unit 29351, APO AE 09014-9351, for approval.

b. If additional IT hardware and software will be needed, the approved request for exception (a above) must be included as part of the information management acquisition request (IMAR) to acquire the hardware and software.

c. The server authorization requirements in paragraph 11 will apply when establishing the system.

d. When a unit is granted an exception, the unit will still be required to maintain a presence on the AKO portal. The unit’s AKO portal must have a hyperlink to the unit’s extranet site.

### **22. ACCESS-CONTROL REQUIREMENTS**

a. When publishing data on the unit AKO portal and KCCs, units must apply “Deny All Permit by Exception (DAPE)” AKO access control to ensure only the authorized audience can access it.

b. If a unit has an approved exception to IOM additional extranet Web servers it will use DAPE to control access to its extranet.

(1) Basic site-level protection will be implemented by using a combination of secure sockets layer (SSL) encryption, public key infrastructure (PKI) authentication, and IP filter to establish protection of data on the site. The basic site-level controls will permit access to the smallest acceptable audience and may be expanded as required by the mission (including approved requests from personnel outside of the basic audience).

**(a) Example 1.** If the information the commander of 1st Infantry Brigade wants to post should be accessible only to personnel outside his organization who are assigned to 1st Armor Division, do not use a combination of access controls that will permit or allow access to all DOD personnel. Instead, use the combination of access controls (IP filter, PKI, login and password) to ensure the information is accessible only to personnel in the 1st Armored Division.)

**(b) Example 2.** The data owner determines information to be posted should be accessible to personnel outside the unit (for example, other Army units, major Army commands, USEUCOM). To support this requirement, use the combination of access controls (PKI, SSL, and IP filter) to ensure the information is accessible only by personnel or units the data owner designates and who have been approved by the commander or designated approval authority.

(2) When a data owner wants to post information to be available to an audience more restricted than defined in b(1) above, the Web master or Web author will use the basic site-level protections in b(1) above and a combination of access controls to ensure the information is released only to the data owner's authorized audience. The key is to use the method that provides access only to the authorized audience (for example, DAPE). This may include a more restrictive IP filter, mapping an individual's PKI certificate to the domain account, using the operating system file permissions (NTFS or Active Directory), AKO single sign-on authentication that provides the required protection, or an internal (database driven) application that provides additional login and password protection.

### **23. APPROVAL PROCESS**

a. Before data owners request approval to publish documents on their extranet, they must—

(1) Determine the sensitivity of the information and develop metadata for the data to be posted (para 8).

(2) Recommend the authorized audience to help establish which offices must review the content and to help the content manager and Web author or Web master determine—

(a) Which Web site (Internet, extranet, intranet) the information should be posted on.

(b) What access controls should be implemented.

b. After completing the steps in subparagraph a above, the data owner will submit the information for approval to the unit content manager. If the content manager has been delegated approval authority by the commander to publish information to private sites, the content manager may direct the Web master or Web author to post the information or may direct the data owner to get unit OPSEC or PAO approval before the information may be posted (if the content manager needs additional clarification). Otherwise, the content manager will request approval from the commander and then provide the Web master or Web author with posting instructions.

### **24. ENCRYPTION STANDARD**

All AE extranet Web sites will use a 128-bit, class 3 DOD medium-level PKI certificate to enable SSL encryption and Web site identification. The name of the certificate must match the name of the basic site (for example, if the site URL is *https://hqusareur-extranet.army.mil*, the name of the certificate must be *hqusareur-extranet.army.mil*). The certificate will not contain the names of lower-level directories in the Web server). The unit will also install the DOD root-level certificates in the server certificate repository.

## **SECTION IV**

### **INTRANET WEB SITES**

#### **25. DEFINITION**

An "intranet Web site" includes IT hardware and Web server software that will enable an organization to share and protect information and applications internally (within the organization). Access is generally restricted to that organization and elements subordinate to it. (For example, the Commander, 1st Brigade, 1st Armored Division, directs the establishment of a Web site for sharing information that will be accessible only to his staff and his subordinate battalions.)

#### **26. ACCESS-CONTROL REQUIREMENTS**

Access-control requirements for intranets are the same as those in paragraph 22 except that the basic access controls will prevent access to the intranet site by anyone who is not assigned to the organization or assigned to a subordinate unit of the organization operating the site or otherwise approved by the unit commander.

#### **27. APPROVAL PROCESS**

The policy and procedures in paragraph 23 apply to the intranet.

#### **28. ENCRYPTION STANDARD**

The policy and procedures in paragraph 24 apply to the intranet.

## **APPENDIX A REFERENCES**

Privacy Act (5 USC 522)

(available at <http://www.usdoj.gov/foia/privstat.htm>)

Freedom of Information Act (5 USC 522a)

(available at <http://www.usdoj.gov/04foia/foiastat.htm>)

Fraud and Related Activity in Connection With Computers (18 USC 1030)

(available at <http://www.usdoj.gov/criminal/cybercrime/1030NEW.htm>)

Rehabilitation Act (29 USC 794d)

(available at <http://www.section508.gov/>)

Executive Order 12958, Classified National Security Information

(available at <http://www.fas.org/irp/offdocs/eo12958.htm>)

National Archives and Records Administrative General Records Schedule 20, Electronic Records

(available at [http://www.archives.gov/records\\_management/ardor/grs20.html](http://www.archives.gov/records_management/ardor/grs20.html))

Memorandum, Office of the Assistant Secretary of Defense, 25 November 1998, subject: Web Site Administration Policies & Procedures

(available at [http://www.defenselink.mil/Webmasters/policy/dod\\_web\\_policy\\_12071998\\_with\\_amendments\\_and\\_corrections.html](http://www.defenselink.mil/Webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html))

Memorandum, Office of the Deputy Secretary of Defense, 24 September 1998, subject: Information Vulnerability and the World Wide Web

(available at [http://www.defenselink.mil/other\\_info/depsecweb.pdf](http://www.defenselink.mil/other_info/depsecweb.pdf))

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

AR 25-2, Information Assurance

AR 25-11, Record Communications and the Privacy Communications System

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

AR 25-400-2, The Army Records Information Management System (ARIMS)

AR 360-1, The Army Public Affairs Program

AR 530-1, Operations Security (OPSEC)

United States Army Installation Management Agency Web Site Administrative Standing Operating Procedure, 11 May 2004

(available from the IMA-E Public Affairs Office)

**APPENDIX B  
PUBLIC AFFAIRS CONTENT APPROVAL CHECKLIST**

**B-1. GENERAL**

Unit public affairs office (PAO) POCs will use the checklist below to review content submitted by data owners for posting on unit Web sites. The result of the review will be a recommendation to the unit commander or content manager to post the information on the unit’s public site (Internet) or private site (intranet or extranet, depending on the audience recommended by the data owner).

1. Is the content free of classified information? (If the answer is “no,” the content will not be posted on any of the unit’s LandWarNet (Unclas) Web sites.)	
2. Is the material free of unclassified sensitive information and not concern intelligence activities, cryptologic activities related to national security, or the command and control of forces? (If the answer is “no,” the information will not be posted on the unit’s public Web site; it may be posted on the unit’s private Web site (either intranet or extranet, depending on the audience).)	
3. Is the content free of records and other information exempt from release under the Freedom of Information Act? This material is For Official Use Only (FOUO). (If the answer is “no,” the information will not be posted on the unit’s public Web site; it may be posted on the unit’s private Web site (either intranet or extranet, depending on the audience).)	
4. Does the content include personal information protected by the Privacy Act? (If the answer is “yes,” the information must not be posted on the unit’s public Web site; it may be posted on the unit’s private Web site (either intranet or extranet, depending on the audience).)	
5. Does the material present a negative image of the Army or the Army in Europe? (If the answer is “yes,” the information will not be posted on any unit Web site.)	
6. Does the content include political commentary or political views? (If the answer is “yes,” the information will not be posted on any unit Web site.)	
7. Is the material intended for a public audience? (If the answer is “no,” it may be posted only on the unit’s intranet or extranet Web site, depending on the audience.)	
8. Is the material free of commercial sponsorship, implied product endorsement, and advertising? (If the answer is “no,” the information will not be posted on any unit Web site.)	
9. Is the content free of sensitive or personal information? (If the answer is “no,” it may be posted only on the unit’s intranet or extranet Web site, depending on the audience.)	
10. Are photographs (if any) in the proper format and resolution? (See para B-2.)	
11. Has the document been “spell checked” and reviewed for punctuation and grammar? (If the answer is “no,” the content will be returned to the data owner for necessary review and corrections.)	

**B-2. PHOTO RESTRICTIONS**

a. Photographic images must be in Joint Photographic Experts Group (JPEG) format and should be 72 dots per inch; graphic images must be in graphic interchange format (GIF) format. JPEG images must be small enough to load quickly using a 28.8 kilobyte (kb) modem. (A 100 kb image needs about 40 seconds to load.) GIF and JPEG image size will depend on the photograph’s intended use. Animated GIF files should be used sparingly.

b. Before considering a photograph to be placed on a public site, ensure that posting the photograph will not violate security regulations or embarrass the Army, the unit, or individuals in the photograph. Consult the commander or PAO to determine whether or not to use certain photographs. Web masters and photographers will enforce the restrictions of AR 360-1, chapter 5, and the following:

(1) Photographs will not include captions that provide the names of family members of soldiers and civilian employees. Captions may identify high-ranking leaders who by virtue of their positions are known to the public.

(2) Photographs of casualties or soldiers in a state of shock or great emotional distress will not be posted on the Internet. Photographs of individuals under medical care in medical facilities require the consent of both the patient and the treating physician (AR 360-1, para 5-32).

(3) Photographs will not show violations of security, safety, propriety, or Army or Army in Europe policy. Examples of photographs that are prohibited are those that show a soldier in any of the following situations:

- (a) Working on a vehicle-brake cylinder without safety glasses, which is a safety violation.
- (b) Performing personal hygiene in underwear, which violates propriety.
- (c) Smoking a cigarette inside a Government building or in a vehicle, which violates Government policy.

### **B-3. AUDIO AND VIDEO**

Audio and video files will be used only when there is a legitimate requirement. Audio and video files must support the organization mission and be appropriate for release using items in the checklist in this appendix. Cartoon audio and video files are not appropriate.

**APPENDIX C  
PUBLIC AFFAIRS WEB SITE REVIEW CHECKLIST**

**C-1. GENERAL**

The checklist in this appendix will be used by unit public affairs office (PAO) POCs to conduct the internal quarterly reviews of their Web sites. The glossary explains abbreviations in the checklist.

1. Does the organization have a clearly defined process for submitting, screening, approving, and posting new Web site content?	
2. Does the organization have a process to conduct quarterly reviews of Web site content?	
3. Does the Web site include a clearly defined purpose statement that supports the mission of the organization?	
4. Are users of each publicly accessible Web site provided a privacy and security notice (para C-2) prominently displayed or announced on at least the first page of all major sections of each Web information service?	
5. If applicable, does this Web site include a disclaimer notice (para C-3) for any site outside of the official DOD Web information service (usually the .mil domain)?	
6. Is the Web site free of commercial sponsorship and advertising?	
7. Is the Web site free of persistent cookies or other devices designed to collect personally identifiable information about Web visitors?	
8. Is each Web site made accessible to users with disabilities according to Section 508 of the Rehabilitation Act?	
9. Each Army in Europe command may have only one public homepage that serves as a virtual “visitor center” for the command. Are the following required items on Army in Europe command homepages?	
Name of the organization or unit?	
Commercial-link disclaimer notice? Army in Europe homepages that have links to NFE Web sites must include or provide a link to the statement in paragraph C-3.	
Date of last update (date the Web site was last updated)?	
Headquarters links? Links to the U.S. Army homepage ( <a href="http://www.army.mil">http://www.army.mil</a> ) and the USAREUR homepage ( <a href="http://www.hqusareur.army.mil">http://www.hqusareur.army.mil</a> ) or IMA homepage ( <a href="http://www.ima.army.mil">http://www.ima.army.mil</a> ). Each organization must also maintain links to its next-higher and next-lower headquarters.	
A link to the SITES system ( <a href="https://www.dmdc.osd.mil/swg/owa/dmdc.home">https://www.dmdc.osd.mil/swg/owa/dmdc.home</a> )? The SITES system provides information on key aspects of the moving process and supplements relocation services provided by relocation-assistance offices on major military installations. This site is updated quarterly based on data received from the various installation relocation-assistance offices. This is one of the most important URLs for a Web site.	
Mission statement or a link from the homepage to the organization or unit mission statement? The unit METL also may be included.	
CPA seal? Displaying the CPA seal shows that the CPA has approved the homepage. The date of approval must be displayed with the seal. IMA-E organizations will use the IMA seal (para 18).	
Privacy and security notice? Homepages must include the notice in paragraph C-2 or provide a link to it. Web pages of major sections of Web sites must provide a link to this notice with the statement “Please read this Privacy and Security Notice.”	
Subordinate units? If subordinate units maintain Web pages, the homepage must list these units and their URLs.	
10. The following are highly recommended to be included in Army in Europe command homepages:	
A JPEG, GIF, or other appropriate graphic that identifies the organization. Each organization should have an appropriate patch or logo that identifies the unit.	
A link to a photograph of the commander with the approved biography. The PAO is responsible for providing the approved biography and photograph. The command sergeant major’s photograph and biography also may be included. Biographies should be limited to the individual’s military and professional record. Family information (such as children’s ages and where they go to school) will not be included.	
A description of the various components of headquarters organizations and its responsibilities. <b>NOTE:</b> Public Web sites must not display rosters that list names of assigned personnel, personal telephone numbers, individual e-mail addresses, or other personal information (such as social security numbers, family member names, home addresses). Web sites may, however, display lists of duty positions, duty telephone numbers, and generic duty e-mail addresses (those constructed by using an abbreviated form of the position title, rather than the name of the person).	
A link to the unit history.	
Unit motto, if the unit has one.	

A link to a section where news releases may be viewed or downloaded with feature stories and photographs. Items must be approved by the PAO before being placed on the Web site (para C-4). Articles must be timely and not left on the page long after the event has taken place.	
Links to other Government Web sites that would be informative and useful to users. A good start is the FirstGov Web site ( <a href="http://firstgov.gov/index.shtml">http://firstgov.gov/index.shtml</a> ), which is an easy-to-search, free-access Web site that may help users find information from other U.S. Government agency Web sites.	
A link to photographs that enhance the Web site (for example, photographs showing the unit perform its mission or train for the mission). The PAO must approve all photographs before they are placed on the Web site (para C-4).	
A list of subordinate units and a description of the mission and history of each.	
The organization vision statement. The vision statement informs users what the organization expects to achieve in the future.	
A link to current weather information. In certain areas, access to weather information is very important. This is recommended only if a noncommercial link can be found.	
A link to a written greeting. This may be accompanied by a short audio recording.	

### C-2. PRIVACY AND SECURITY NOTICE

The following statement (or a link to it) will be included on all homepages and major sections of Web sites:

1. This site is provided as a public service by (organization name).
2. Information on this site is considered public information and may be distributed or copied for noncommercial purposes. Use of appropriate byline, photograph, and image credits is requested.
3. For site management, information is collected for statistical purposes. This Government computer system uses software programs to create summary statistics that are used for purposes, such as assessing what information is of most and least interest, determining technical-design specifications, and monitoring system performance and problem areas.
4. For site-security purposes and to ensure that this service remains available to all users, this Government computer system uses software programs to monitor network traffic to identify unauthorized attempts to upload or change information or otherwise cause damage.
5. Except for authorized law-enforcement investigations, no other attempts are made to identify individual users or their habits when using the Web site. Raw-data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration General Records Schedule 20.
6. Unauthorized attempts to upload or change information on this system are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.

### C-3. DISCLAIMER

The following statement (or a link to it) must be included on all pages that have links to NFE Web sites:

The appearance of this link does not constitute endorsement of the Web site or the information, products, or services contained therein by the U.S. Army. For other than authorized activities, the Army does not exercise any editorial control over the information that may be found at this link. This link is provided in accordance with the stated purpose of this military Web site.

### C-4. PHOTOGRAPHIC AND GRAPHIC IMAGES

**a. Format.** Photographic images must be in Joint Photographic Experts Group (JPEG) format and should be 72 dots per inch. Graphic images must be in graphic interchange format (GIF) format. JPEG images must be small enough to load quickly using a 28.8 kilobyte (kb) modem. (A 100 kb image needs about 40 seconds to load.) GIF and JPEG image size will depend on the photograph's intended use. Animated GIF files should be used sparingly.

**b. Requirements.** Photographs that support Army public information and similar programs may appear on the Internet. These include photographs of soldiers and civilian employees performing duties or participating in recreational activities (such as unit sporting events). Photographs must be limited to those that show soldiers and civilian employees in situations that accurately represent Army activities, missions, and uniforms.

(1) Photographers should inform subjects of photographs that the picture might appear on the Internet. If someone objects to his or her picture appearing on the Internet, the person will not be photographed.

(2) Photographs taken in Department of Defense Dependents Schools, Army and Air Force Exchange Service facilities, and commissaries generally require the consent of the agency responsible for the facility where the photograph is to be taken.

(3) Photographs of individuals in hostile areas generally require formal consent and authorization to publish (AR 360-1, para 5-31).

**c. Restrictions.** Before placing a photograph on the Internet, the Web master must ensure that posting the photograph will not violate security regulations or embarrass the Army, the unit, or individuals in the photograph. The Web master may need to consult the commander or PAO to determine whether or not to use certain photographs. Web masters and photographers will enforce the restrictions of AR 360-1 and the following:

(1) Photographs will not include captions that provide the names of family members of soldiers and civilian employees. Captions may identify high-ranking leaders who by virtue of their positions are known to the public.

(2) Photographs of casualties or soldiers in a state of shock or great emotional distress will not be posted on the Internet. Photographs of individuals under medical care in medical facilities require the consent of both the patient and the treating physician (AR 360-1, para 5-32).

(3) Photographs will not show violations of security, safety, propriety, or Army or Army in Europe policy. Examples of photographs that are prohibited are those that show a soldier in any of the following situations:

(a) Working on a vehicle-brake cylinder without safety glasses, which is a safety violation.

(b) Performing personal hygiene in underwear, which violates propriety.

(c) Smoking a cigarette inside a Government building or in a vehicle, which violates Government policy.

#### **C-5. AUDIO AND VIDEO**

Audio and video files will be used only when there is a legitimate requirement. Audio and video files must support the organization mission and be appropriate for release on the Internet. Cartoon audio and video files are not appropriate.

**APPENDIX D  
OPSEC WEB SITE REVIEW CHECKLIST**

**D-1. GENERAL**

a. The unit operations security (OPSEC) POC will use the checklist in this appendix to conduct the unit’s internal quarterly Web site review. The unit OPSEC POC will also use all paragraphs except those under section I (Controls) to review information that is being submitted by a data owner for posting. A “yes” answer for any of the items in sections II and III indicates that the information may not be posted on a publicly accessible site and that proper access controls must be established for posting on the unit’s private site (intranet or extranet as determined by the data owners audience).

b. The checklist is generic. There are many other indicators possible for military operations and activities. The checklist does not provide every consideration needed for a complete organizational OPSEC program.

**D-2. INFORMATION SECURITY**

In the context of information assurance, the World Wide Web should not be treated any differently from any other potentially vulnerable system. Security of information on publicly accessible Web sites must be viewed as part of an organization’s overall OPSEC posture.

Name:	Date/Time of Review:		
Organization Reviewed:	Primary IP Address/URL:		
<i>Issue/Concern</i>	<i>Yes</i>	<i>No</i>	<i>Notes/Comments</i>
<b>Section I. Controls</b> (note 1)			
1. Does the Web site include a clearly defined purpose statement that supports the mission of the Army in Europe or subordinate units?			
2. Is a privacy and security notice prominently displayed or announced on at least the first page of all major sections of each Web information service?			
3. If applicable, does the Web site include a disclaimer for external links when a user requests any site outside of the official DOD Web information service (usually the .mil domain)?			
4. Is this Web site free of commercial sponsorship and advertising?			
<b>Section II. Guidance</b> (note 2)			
<b>1. Operational Information.</b> Does the Web site or content include—			
a. Any information indicating plans or lessons learned that would reveal military operations, exercises, or vulnerabilities?			
b. Any reference to information that would reveal sensitive movements of military assets or the location of units, installations, or personnel where uncertainty about location is an element of the security of a military plan or program?			
<b>2. Personal Information.</b> Does the Web site or content include personal information in the following categories about U.S. citizens, DOD employees, or military personnel?			
a. Social security account numbers.			
b. Dates of birth.			
c. Home addresses.			
d. Home telephone numbers.			
e. Names, locations, or other identifying information about family members.			
<b>3. Technological Data</b> (note 3). Does the Web site include any technical data, such as the following?			
a. Weapon schematics.			
b. Weapon system vulnerabilities.			
c. Electronic wire diagrams.			
d. Frequency spectrum data.			

**Section III. OPSEC Considerations: "Tip Off Indicators" (note 4)**

Does the Web site or content include relevant information in the following categories that might reveal an organizations plans and intentions based on the current critical information list?

<b>1. Administrative:</b>			
a. Personnel travel (personal and official business).			
b. Attendance at planning conferences.			
c. Commercial support contracts.			
<b>2. Operations, Plans, and Training:</b>			
a. Operation orders and plans.			
b. Mission-specific training.			
c. Exercise and simulations activity.			
d. Exercise, deployment, or training schedules.			
e. Unit relocation or deployment.			
f. Inspection results, findings, deficiencies.			
g. Unit vulnerabilities or weaknesses.			
h. Force-protection conditions or measures.			
<b>3. Communication:</b>			
a. Radio frequency emissions and associated documentation.			
b. Changes in activity or communications patterns.			
c. Use of Internet or e-mail by unit personnel (personal or official business).			
d. Availability of secure communications.			
e. Hypertext links with other agencies or units.			
f. Family support plans.			
g. Bulletin board or messages between soldiers and family members.			
<b>4. Logistics/Maintenance:</b>			
a. Supply and equipment orders or deliveries.			
b. Transportation plans.			
c. Mapping, imagery, and special documentation support.			
d. Maintenance and logistics requirements.			
e. Receipt or installation of special equipment.			

**Section IV. Key Word Search**

Use the following key words to conduct a search of Web sites. Use the results of the search to conduct a random screen for unauthorized content.

a. Biographies			
b. Contingency plans			
c. Deployment schedules			
d. Exercise plans			
e. Family support activities			
f. Force protection information			
g. Inspection results, findings, deficiencies			
h. Telephone directories or lists			
i. Training schedules			

**NOTES:** 1. These controls are in the policy published by the Office of the Assistant Secretary of Defense, 25 November 1998, subject: Web Site Administration Policies & Procedures.  
 2. The items in this section were copied from Memorandum, Office of the Deputy Secretary of Defense, 24 September 1998, subject Information Vulnerability and the World Wide Web.  
 3. Technical data creates a unique challenge to the OPSEC posture of an organization and to national security. Certain technical data, when compiled with other unclassified information, may reveal an additional association or relationship that meets the standards for classification under Executive Order 12958, section 1.8(e).  
 4. "Tip-off indicators" are listed in AR 530-1. Tip-off indicators highlight information that otherwise might pass unnoticed. These are most significant when they warn an adversary of impending activity. This allows the adversary to pay closer attention and to use additional collection assets.

**APPENDIX E  
INFORMATION INFRASTRUCTURE ASSISTANCE TEAM INSPECTION CHECKLIST**

**NOTE:** The glossary explains abbreviations used in the checklist.

<b>Item</b>	<b>Compliance</b>	<b>Remarks/Action Required</b>	<b>End of Assessment</b>
<b>Section I</b>			
1. Do private Web servers (intranet or extranet) use SSL protocol through a class 3, medium-grade PKI certificate issued by the DOD PKI key agent?			
2. Does the name of the certificate match the name of the root level of the site?			
3. Has the site installed the DOD root level certificates?			
4. Do private Web servers have PKI authentication enabled at the site level?			
5. Do private Web servers have the server IP filter enabled at the site level to restrict access to authorized IP networks?			
6. Are FOUO and other sensitive documents protected with additional access controls to ensure the need-to-know rule has been applied according to the data owner's audience requirement?			
<b>Section II</b>			
7. Have the commander or content manager, PAO, OPSEC, and other appropriate offices properly cleared information posted on unit Web sites?			
8. Has the unit commander (or civilian equivalent) designated on duty appointment orders an OPSEC POC, PAO POC, content manager, and either a Web master (in the nonconsolidated environment) or Web author (in the consolidated environment) for the unit?			
9. Has the unit content manager completed the AE content manager's course?			
10. Has the unit Web master or Web author completed all of the required training to be AE certified?			
<b>Section III</b>			
11. Is documentation maintained to show that required approvals for posting information have been obtained?			
<b>Section IV</b>			
12. Do unit Web sites comply with Section 508, priority 1?			
13. Does the unit use the handicap-accessibility icon to designate compliance?			
14. Has the unit completed all quarterly internal reviews, resolved deficiencies, and documented the review in official unit records?			
15. Has the unit defined all content and pages using the metadata standard?			
16. Does the unit operate a portal page and KCCs on the AKO portal as its primary extranet Web site?			
17. Is posted information current?			
18. Does the unit possess a valid exception from the USAREUR G6 to operate an additional extranet application in addition to the AKO portal page?			

Item	Compliance	Remarks/Action Required	End of Assessment
19. Does the unit have a functional data backup procedure that completes a full back up at least once each week and an incremental backup once each day?			
20. In the consolidated environment, does the server manager provide required access to the server to enable the Web author to appropriately add content and required security access controls?			
21. Are the privacy and security notices posted in a prominent location on at least the first page of all major sections of each public Web site?			
22. Are the following types of restricted information on the public Web site?			
a. Classified information.			
b. Unclassified information concerning intelligence activities, cryptologic activities related to national security, or the command and control of forces.			
c. Records and other information that is exempt from release under the FOIA (FOUO material).			
d. Material that presents a negative image of the Army.			
e. Personal information protected by the Privacy Act.			
<b>Section V</b>			
23. Are the following types of restricted information on the public Web site?			
a. Command title.			
b. Commercial link disclaimer notice (if applicable).			
c. Date of last update.			
d. Headquarters links (U.S. Army and USAREUR or IMA).			
e. Housing and community information (link to SITES).			
f. Mission statement.			
g. CPA or IMA seal.			
h. Privacy, security, and data-collection notices.			
i. Links to subordinate unit Web pages.			

**APPENDIX F  
AE METADATA TAG STANDARD**

**Unclassified Metadata Tagging Standard Format**

<b>Title</b>	<input type="text"/>	<b>Description</b>	<input type="text"/>
<b>Creator</b>		<b>Security</b>	
Organization	<input type="text"/>	Sensitivity	<input type="text" value="Not sensitive"/> <input type="text" value="FOUO"/> <input type="text" value="Privacy Act"/>
Office Symbol	<input type="text"/>	Dissemination	<input type="text" value="Contact originating office"/> <input type="text" value="Authorized U.S. Government agencies"/> <input type="text" value="Authorized U.S. Government agencies and their contractors"/>
Telephone No.	<input type="text"/>		
<b>Dates</b>		<b>Location Information</b>	
Date Created	<input type="text"/>	Location Created	<input type="text" value="GERMANY"/> <input type="text" value="AFGHANISTAN"/> <input type="text" value="AZERBAIJAN"/>
Date Posted	<input type="text"/>	Region Created	<input type="text" value="AFRICA"/> <input type="text" value="CENTRAL AMERICA"/> <input type="text" value="EUROPE"/>
Date Valid To	<input type="text"/>		
Date Info Cutoff	<input type="text"/>		
<b>Subject</b>			
Keywords	<input type="text"/>		
Subject Codes	<input type="text"/>		
Identifier	<input type="text" value="Qualifier URL"/>		

<b>Title</b>	
Requirement	Mandatory.
Description	Typically, a title will be a name by which the resource is formally known.
XML	<title> Department of Defense Discovery Metadata Standard (DDMS) </title> <subtitle> Review Version 1.2 </subtitle>
<b>Creator</b>	
Requirement	Mandatory.
Description	Information about the entity responsible for generating the resource.
Comment	When a creator is a service or an organization (not an individual), it is expected that the contact authority (person or organization) for the resource will be listed.
<b>Organization</b>	Values in this element should indicate whether the other mandatory creator elements relate information pertaining to an author, point of contact, or organization.
<b>Office Symbol</b>	The office symbol of an organization or agency with which an individual or service is affiliated.

<b>Telephone No.</b>	This value must include country code or area code, when applicable.
XML	<pre>&lt;creator&gt;&lt;XML&gt;&lt;creator qualifier="organization"&gt; &lt;affiliation&gt;U.S. Army&lt;/affiliation&gt; &lt;officesymbol&gt;AEAIM-C-P&lt;/officesymbol&gt; &lt;phonenum&gt;222-222-2222&lt;/phonenum&gt; &lt;/creator&gt;&lt;/XML&gt;</pre>
<b>Date</b>	
Comment	<p>The recommended practice is to specify the date in one of the following formats:</p> <p>YYYY  YYYY-MM  YYYY-MM-DD  YYYY-MM-DDThh:mmTZD  YYYY-MM-DDThh:mm:ssTZD  YYYY-MM-DDThh:mm:ss.sTZD</p> <p>Where:</p> <p>YYYY 0000 through current year  MM 01 through 12 (month)  DD 01 through 31 (day)  hh 00 through 24 (hour)  mm 00 through 59 (minute)  ss 00 through 60 (second)  .s .0 through 999 (fractional second)</p> <p>There are two ways of identifying the time-zone:</p> <ol style="list-style-type: none"> <li>Expressing time in UTC (Coordinated Universal Time), with a special UTC designator ("Z").</li> <li>Expressing time in local time with a time-zone offset in hours and minutes. A time-zone offset of "+hh:mm" indicates that the date/time uses a local time zone which is "hh" hours and "mm" minutes ahead of UTC. A time-zone offset of "-hh:mm" indicates that the date/time uses a local time zone which is "hh" hours and "mm" minutes behind UTC.</li> </ol>
<b>Date Created</b>	Date product was created.
Requirement	Mandatory.
<b>Date Posted</b>	The date a product is posted to a shared network or system.
Requirement	Optional.
<b>Date Valid To</b>	The date that a product should be reviewed for removal from a registry, index, or catalog. The default is 6 months after the date created.
Requirement	Mandatory.
<b>Date Info Cutoff</b>	<p>The cutoff date of information in a product. This must be one of the following:</p> <ul style="list-style-type: none"> <li>• K – Keep for 6 years or less after date created.</li> <li>• KE – Keep for 6 years or less after a specific event (provide event date).</li> <li>• T – Keep more than 6 years after date created.</li> <li>• TE – Keep for more than 6 years after a specific event (provide event date).</li> </ul>
Requirement	Mandatory.
XML	<pre>&lt;date&gt; &lt;datecreated&gt;2003-02-17&lt;/datecreated&gt; &lt;dateposted&gt;2003-02-17&lt;/dateposted&gt; &lt;datevalidtil&gt;2003-02-17&lt;/datevalidtil&gt; &lt;dateinfocutoff&gt;2001-10-31T17:00-05:00&lt;/dateinfocutoff&gt; &lt;/date &gt;</pre>
<b>Subject</b>	
<b>Keyword</b>	Keywords, key phrases, or classification codes that describe a topic of the resource. The recommended practice is to select a value from a controlled vocabulary or formal classification scheme. This may list keywords that apply to the resource or a particular subject category that will help the user understand what the content is about.
Requirement	Optional.

XML	<subject> <keyword>missile</keyword> <keyword>targeting</keyword> </subject>
<b>Subject Codes</b>	A list of codes selected from a provided list.
Requirement	Mandatory.
XML	<subject> <subjectcode>missile</subjectcode> <subjectcode>targeting</subjectcode> </subject>
<b>Identifier</b>	An unambiguous reference to the resource in a given context. An internal, external, or universal identification number for a data asset or resource.
Requirement	Mandatory.
XML	<identifier qualifier="URL">http://www.dod.mil/index.html</identifier>
<b>Description</b>	
Requirement	Optional.
Description	May include (but is not limited to) an abstract, a reference to a graphical representation of content, or a free-text account of the content.
XML	<description> Example -This publication is an analysis of the logistics of re-supplying the cave complex at Tora Bora. </description>
<b>Security</b>	
Requirement	Mandatory.
Comment	This standard is only for unclassified information.
<b>Sensitivity</b>	Must be one of the following: <ul style="list-style-type: none"> <li>● Not sensitive</li> <li>● FOUO</li> <li>● Privacy Act</li> </ul>
<b>Dissemination</b>	Must be one of the following: <ul style="list-style-type: none"> <li>● Contact originating office</li> <li>● Authorized U.S. Government agencies</li> <li>● Authorized U.S. Government agencies and their contractors</li> </ul>
XML	<security> <classification>Unclassified</classification> <disseminationcontrols>FOUO</disseminationcontrols> <releasableto>U.S. ARMY and MITRE</releasableto> </security>
<b>Location Information</b>	
Requirement	Mandatory.
<b>Location Created</b>	A specific identification number or point location. This will be selected from a provided facility location table.
<b>Region Created</b>	The name of a subnational or transnational geographic or geopolitical region that is a subject of the product. This will be selected from a provided country region table.
XML	<geospatial> <facility BE number>GE12F Campbell Barracks</facility BE number> <region>Europe</region> </geospatial>

## GLOSSARY

### SECTION I ABBREVIATIONS

1st IOC	1st Information Operations Command
AE	Army in Europe
AKM	Army Knowledge Management
AKO	Army Knowledge Online
ASG	area support group
CPA	Chief, Public Affairs, USAREUR
DA	Department of the Army
DAPE	Deny All Permit by Exception
DOD	Department of Defense
dpi	dots per inch
FOUO	For Official Use Only
GIF	graphic interchange format
HQ USAREUR/7A	Headquarters, United States Army Europe, and Seventh Army
HTML	HyperText Markup Language
I2AT	Information Infrastructure Assistance Team
IA	information assurance
IACND	information assurance and computer network defense
IMA	United States Army Installation Management Agency
IMA-E	United States Army Installation Management Agency, Europe Region Office
IMAR	information management acquisition request
IOM	install, operate, and maintain
IP	Internet protocol
IT	information technology
ITSA	Information Technology Support Activity
JPEG	Joint Photographic Experts Group
kb	kilobyte
KCC	knowledge community center
METL	mission-essential task list
MSC	major subordinate command
NFE	non-Federal entity
NSC	network service center
NTFS	New Technology File System
OPSEC	operations security
PAO	public affairs office
PKI	public key infrastructure
POC	point of contact
RCERT	Regional Computer Emergency Response Team
SITES	Standard Installation Topic Exchange Service
SOP	standing operating procedure
SSL	secure sockets layer
SSSA	system security authorization agreement
STAMIS	Standard Army Management Information System
URL	uniform resource locator
USAREUR	United States Army, Europe
USEUCOM	United States European Command
USC	United States Code
UTC	Coordinated Universal Time

### SECTION II TERMS

#### **Army in Europe**

All USAREUR and IMA-E organizations and personnel.

**extranet Web site**

Information technology, including hardware and Web server software, that provides protected, limited, or restricted access to information that will be shared outside of the organization but not with the public at large.

**Internet Web site**

Information technology, including hardware and Web server software, that provides access to publicly releasable information through the World Wide Web. Information placed on an Internet Web site can normally be accessed by any computer system connected to the Internet. The Chief, Public Affairs, USAREUR; and Information Technology Support Activity operate the only authorized Internet (public) Web server hardware for USAREUR units. IMA-E organizations will use the IMA public server.

**intranet Web site**

Information technology, including hardware and Web server software, that will enable an organization to share and protect information and applications internally (within the organization). Access is generally restricted to that organization and elements subordinate to it.

**metadata**

Information about a data owner's information that defines the document (for example, what the document is about, sensitivity of the information, expiration date). Metadata allows information to be indexed and searched more accurately. Metadata may be included as part of the template in the document or coded into HTML pages.

**Web server**

The information technology hardware (computer) and software (operating system and application) that can be configured to install, operate, and maintain one or many Web sites.

**Web site**

HyperText Markup Language (HTML) code and information created by a unit to be shared with a designated audience on the Internet or through an intranet or extranet.