



COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO WWW site at:
<http://www.e-publishing.af.mil>

OPR: HQ USAFE/SCNI
(MSgt Gregory J. Krzyzanowski)
Supersedes AFI 33-129, USAFE Supplement 1,
29 August 2000.

Certified by: HQ USAFE/SCN
(Col Michael Q. Harper)
Pages: 9
Distribution: F

AFI 33-129, 4 April 2001, is supplemented as follows: This supplement applies to all United States Air Forces in Europe (USAFE) units within the theater. It also applies to Air National Guard and Air Force Reserve members when deployed or assigned to the theater. This supplement prescribes USAFE Form 883, Request for Review of Internet Release Package, and USAFE Form 884, Web Site Quarterly Review Log. Units may establish local supplements to create more stringent control, according to AFI 36-360, Volume 1, *Publications Management Program*. All local supplementation must be coordinated with (USAFE/SCNI). Maintain and dispose of records created as a result of prescribed processes according to AFMAN 37-139, *Records Disposition Schedule*.

SUMMARY OF REVISIONS

This change clarifies the role of the Computer Systems Squadron, Network Operations Security Center, Enterprise Application Branch (USAFE CSS/SCNOE) in hosting and maintaining the commands consolidated server farm. Paragraph 3.6. establishes HQ USAFE directors' responsibilities. The revision refines Information Not Appropriate for Public Release (see paragraphs 7.4.10. and 7.4.11.). Revisions have been marked with vertical bar (|) in left margin.

3.4.1. Internal Information Division (HQ USAFE/PAI) approves and reviews publicly accessed web sites according to guidance provided at **Attachment 5 (Added)** *Internet Release Package Procedures*.

3.6. HQ USAFE directors are considered "commanders" for the purpose of executing responsibilities in this instruction and supplement.

3.6.5. (Added) Appoint a web page maintainer, in writing, and forward the appointment letter to the web server administrator. Web page maintainers must be able to perform their duties without jeopardizing security or violating legal statutes. Training requirements include, but are not limited to, completion of computer-based training courses: *A Beginner's Guide to Hypertext Markup Language (HTML)*, *Web*

Authoring and Publishing: HTML Documents; Web Authoring and Publishing: Web Site Presentation; and Web Authoring and Publishing: Building Fill-In Forms that may be obtained at web site <https://wwwmil.usafe.af.mil/pagemaintainer>. Page maintainers must also review AFI 33-129; AFI 33-129, USAFE Supplement 1; and local policies (obtained from the communications squadron). Attending the Introduction to Web Programming for Page Maintainers Course at the USAFE Communications Information Training Center and receiving local training provided by the base communications squadron also meets the training requirements. USAFE CSS/SCNOE can assist with the development of a local training program.

3.8.5. Establish one limited access (“mil” accessed) site, which will be hosted on consolidated command Web server farm. USAFE CSS/SCNOE will manage the command’s public sites and limited access sites on consolidated server farms located at Ramstein AB Germany.

3.8.6. (Added) USAFE CSS/SCNOE conducts monthly audits to locate unauthorized public-access web servers and unapproved limited-access web servers. For unauthorized public-access web servers, contact the responsible information provider or office of primary responsibility (OPR), move data to the HQ USAFE consolidated web server (maintained by USAFE CSS/SCNOE), and take action to disconnect the unauthorized public-access server from the network. Authorized limited-access web servers that cannot be accessed from outside the base boundary protection should not be migrated to the HQ USAFE web servers. Take appropriate action to ensure the network and the information is protected.

3.10.2. Notify the web page point of contact and the unit’s operation security (OPSEC) monitor if sensitive information or security risks are found.

3.11. The information provider and the OPR are the same (see paragraph 7 of the basic instruction).

3.13.5. The base public affairs office will lead a multidisciplinary review board for subordinate public web sites. Agencies will process requests through the local public affairs office to HQ USAFE/PAI via fax DSN 480-2705 or e-mail: <mailto:usafe.pai@ramstein.af.mil>.

3.14. The Public Affairs Office (HQ USAFE/PA) leads and facilitates the command’s multidisciplinary review boards. The board convenes as often as necessary, but at least once annually.

4.1.1.1. The Public Affairs Office (USAFE/PA) maintains top-level home page for publicly accessed pages. USAFE CSS/SCNOE maintains USAFE’s top-level home page; the base communications squadrons maintain the top-level home pages for base level home page for the limited-accessed pages.

4.1.1.15. (Added) USAFE CSS/SNOE verifies that all page maintainers are trained prior to granting access to the web server. Ensure all page maintainers successfully complete USAFE Page Maintainer quiz.

4.2.1.2. The information provider or OPR documents release authority according to AFI 33-129, see paragraph 7.5. of this supplement. In some cases, USAFE will agree to host web sites or pages for non-USAFE organizations or tenant units. In this situation, the OPR from the non-USAFE organization must provide documented approval from their commander or designated representative.

4.2.1.9. (Added) Ensuring pages and links are reviewed and updated at least every 90 days. Document this review by updating the “Date Last Reviewed” entry of the web pages and entering the date, name and signature of the individual completing the review on USAFE Form 884, **Web Site Quarterly Review Log**, maintained with the original Internet Release Package.

6.1. Commanders may delegate, in writing, the authority to authorize use of government-provided resources to further professional and military knowledge of their personnel to the lowest appropriate level.

6.4. Wing commanders may authorize appropriated funds for commercial internet service provider (ISP) service to family support centers and morale, welfare, and recreation (MWR) mission sustaining activities (Category A) and basic community activities (Category B) according to AFI 36-3009, *Family Support Center Programs*, and AFI 65-106, *Appropriated Fund Support of Morale, Welfare, and Recreation and Non-Appropriated Fund Instrumentalities*. MWR Revenue Generating Activities (Category C) are typically not permitted commercial ISP service with appropriated funds. Wing commanders will establish commercial ISP approval and management procedures through their communications unit to ensure cost effective service to all users.

6.4.1. (Added) Do not put government-provided ISP services to any use that would reflect adversely on the United States Air Force or Department of Defense (DoD). Such use involves pornography, chain letters, unofficial advertising, soliciting, or violations of statutes or regulations. Notify non-mission-related users, via banner, that use of government-provided ISP service by authorized users constitutes consent to have all communications monitored for security and management purposes according to AFI 33-129 and AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*.

6.4.1.1. (Added) Unauthorized use by individuals not employed by the US government may result in restrictions on access to service, termination of service, and other administrative penalties, including reimbursement to the government for additional costs that may be incurred, without regard to otherwise applicable criminal or civil sanctions for violations of related laws.

6.5. (Added) US government employees (i.e., US military members and US civilian employees) assigned to North Atlantic Treaty Organization (NATO) billets and DoD contractors are permitted Internet or e-mail access, using the US military network ("af.mil" domain) and US government exclusively owned communications systems and equipment, for official and authorized purposes only.

6.5.1. (Added) If the DoD contractor is required to perform certain tasks via the Internet or e-mail, the US organization utilizing the contractor identifies and justifies access requirement according to contract procedures. Background investigations must be completed prior to granting access to the ".mil" network.

6.5.2. (Added) All DoD contractors and US government employees will comply with command and local standards relating to use of the Internet and e-mail.

6.5.3. (Added) Commanders will immediately terminate access for individuals suspected of fraud, waste, or abuse, and notify the command, control, communications, and computers (C4) systems officer (CSO) and contracting officer if appropriate.

7.1. Unclassified information must be reviewed by HQ USAFE staff directors, unit commanders, or their designated representative prior to placing it on the web server. If Controlled Unclassified Military Information (CUMI) is included on the web site, the information must also be approved for release by the Foreign Disclosure Office (USAFE/FDO). If it is unclear whether CUMI is contained in the submission, use caution and send it to the FDO for approval. Once approved, follow procedures outlined in **Attachment 4 (Added)** for both public and limited access sites.

7.2.1.3. (Added) DoDD 5400.7-R, Jun 02, *DoD Freedom of Information Act (FOIA) Program*, requires records determined likely to be subject to frequent FOIA requests be placed in a FOIA Reading Room on the public server. The local FOIA Office (HQ USAFE/SCYI) manages the FOIA Reading Room and the

link to the Air Force FOIA web site at <http://www.foia.af.mil>. The FOIA Officer, with the coordination of the functional OPR or the owner of the records, will determine whether records qualify for posting on the FOIA Reading Room. The FOIA Officer will obtain the appropriate legal reviews where required from the Office of the Staff Judge Advocate.

7.2.2. **Attachment 4 (Added)** contains a sample staff summary sheet to request approval from HQ USAFE/PAI to release information via a public site. **Attachment 4 (Added)** outlines procedures for information released to the public through the Internet.

7.4.9. (Added) Link or post biographies of general officers, wing commanders, or command chief master sergeants and equivalents only to the restricted (.mil) sites.

7.4.10. (Added) Items not appropriate for posting to public sites include, but are not limited to, rosters, organizational charts, and directories with names and e-mail addresses; biographies and photos. Products originated and approved by public affairs offices are not covered by this policy (i.e. releases and photos as they pertain to news).

7.4.11. (Added) The posting of individual names, duty information, biographies and photos of personnel who by nature of their position and duties, frequently interact with the public (i.e. general officers and equivalents, Wing CC, CV, and Command Chief Master Sergeants) is authorized. Coordination for postings of this nature will be done through wing public affairs offices. Personal information is exempt from public disclosure and will not be posted on public web sites. Personal information includes names, e-mail addresses, home addresses, telephone numbers, social security numbers, and other information of a private or nonpublic nature.

7.4.12. (Added) Notices of a one-time event, such as a conference or meeting, may also include the project officer's name, duty telephone number, and project e-mail address.

7.5. Documentation will consist of USAFE Form 883, **Request for Review of Internet Release Package**, coordinated by agencies indicated on form and authenticated by the release authority (identified in AFI 33-129 paragraph 7.1) with the appropriate Internet Release Package attached (see **Attachment 4 (Added)**). Routinely updated information does not require release authority review after initial approval unless additions or changes significantly alter the information. OPRs must initiate Internet Release Packages for web sites that existed prior to the publication date of this supplement. OPR will attach proposed web site information in text file format or include link to the draft site. Coordinate the release package via e-mail or paper. Attach e-mail coordination to the file copy of the release package.

8.1.1. Do not partition a server to separate public information from limited-access information. Follow procedures established in paragraph **3.8.5.**

11.1.2.3. Ensure browsers on US government-owned equipment or -operated on US government-owned networks have security features activated.

11.1.3. Do not download anti-virus signature files, software patches, and other similar files from the Internet, i.e., Norton Antivirus Updates, Microsoft Service Packs, etc. Updates must be received through Air Force Computer Emergency Response Team (AFCERT) channels.

12. Web page must be consistent with guidance provided by USAFE CSS/SCNOE and base public affairs office. Do not use unnecessary graphics, video clips, sound clips, or scripts that slow processing time. Limit the use of information that is available at other web sites. However, include links to these sites instead of duplicating the information when required.

12.3. Organizational e-mail address only.

12.5. (Added) **Date of latest page revision.**

19. (Added) **USAFE Forms Prescribed:**

19.1. (Added) USAFE Form 883, **Request for Review of Internet Release Package.**

19.2. (Added) USAFE Form 884, **Web Site Quarterly Review Log.**

Attachment 1 (Added)**GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION*****References (Added)***

DoDD 5400.7-R, Jun 02, *DoD Freedom of Information Act (FOIA) Program*

AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*

AFI 35-101, *Public Affairs Policies and Procedures*

AFI 36-3009, *Family Support Center Programs*

AFI 65-106, *Appropriated Fund Support of Morale, Welfare, and Recreation (MWR) and Non-appropriated Fund Instrumentalities*

Abbreviations and Acronyms (Added)

AFCERT—Air Force Computer Emergency Response Team

COS—C4 Systems Officer

ISP—Internet Service Provider

NOSC—Network Operations Security Center

USAFE—United States Air Forces in Europe.

Terms (Added)

Controlled Unclassified Military Information (CUMI)—Information that could be used to design, develop, engineer, test, produce, manufacture, operate, maintain, overhaul, or modify defense articles.

Attachment 4 (Added)

SAMPLE STAFF SUMMARY SHEET

A4.1. Use the following sample AF Form 1786, Staff Summary Sheet, when submitting request to USAFE/PAI for Public Internet Release Package.

Figure A4.1. Sample Staff Summary Sheet for Public Internet Release Package.

Subject: A--(OFFICE SYMBOL)--PROPOSED USAFE PUBLIC ACCESS WEB SITE
 426IG/DOO Coord
 HQ USAFE/LGC Coord
 HQ USAFE/JAM Coord
 HQ USAFE/SCM Coord
 HQ USAFE/PAI Appr
 COORDINATING OFFICES: SEND REPLY TO USAFE/PAI FOR RETENTION
 -----STAFF SUMMARY

AO:

Suspense:

Tracking #:

1. **PURPOSE:** The purpose of this staff summary sheet is to obtain cross-functional coordination and PAI approval of the proposed or revised publicly accessible web page at Tab 1.
2. **BACKGROUND:** Provide information regarding the purpose of the web page and its intended audience. State that the information on the proposed web site complies with the USAFE Web Page Review Checklist (Tab 2).
3. **RECOMMENDATION:** Recommend cross-functional coordination and PAI approval of the web site at Tab 1.

DESIGNATED RELEASE AUTHORITY NAME, Rank, USAF

Title

2 Tabs

1. Public Web Site Internet Release Package

2. Proposed Web Site Information or Link to Draft Site

------(TAB 1 Public Web Site Internet Release Package)

*Public Web Site Internet Release Package

------(TAB 2 Proposed Web Site Information or Link to Draft Site)

A4.2. Attach proposed web site information in text file format or include link to draft site.

Attachment 5 (Added)

INTERNET RELEASE PACKAGE PROCEDURES

A5.1. Public Web Site Procedures. The web site OPR must initiate an Internet Release Package and maintain approval for information posted to an internet site for each web site maintained. This package will consist of coordination and approval from key agencies and completion of the Web Page Checklist indicated on USAFE Form 883.

A5.1.1. The web site OPR identifies pertinent page data in Section 1 of USAFE Form 883.

A5.1.2. The web site OPR creates an outline of the pages of the web site. This is intended to help reviewers decide which pages they need to review. Specifically, the outline will show all the pages of the web site with a summary of the information on each page. For example, you may use “Unit COMPUSEC Managers Listing” rather than putting the actual listing on the outline or “Information Assurance Publications” rather than showing all the actual files to be available for download.

A5.1.3. The web site OPR must provide the pages of the web site to reviewing officials upon request. Paper or electronic media satisfies this requirement.

A5.1.4. The web site OPR forwards the package to required reviewing officials IN TURN with the OPR’s unit address listed last. Reviewing officials include, minimally, the unit OPSEC Monitor, unit Top-Level Page Maintainer, unit commander, Freedom of Information Act and Privacy Act Monitor or Records Manager, and the local public affairs office. The public affairs office forwards the approved package for cross-functional review to HQ USAFE/PAI (via e-mail: <mailto:usafe.pai@ramstein.af.mil> or fax DSN: 480-2705), see Attachment 3 (Added). Once approved, HQ USAFE/PAI posts information to the USAFE-centralized public web server. The OPR resolves issues causing nonconcurrence by any reviewer. Agencies should use the following guide to determine whether the information is releasable. However, the concerns for review are not all inclusive.

A5.1.4.1. The Unit OPSEC monitor reviews web sites to ensure it does not provide information of possible intelligence value nor create an OPSEC vulnerability.

A5.1.4.2. The organization’s top-level page maintainer reviews the site for compliance with AFI 33-129 and any existing local standards.

A5.1.4.3. The unit commander reviews the package to ensure the associated risks that arise by posting the information are outweighed by the necessity to have the information readily and easily accessible by its intended audience.

A5.1.4.4. The local Freedom of Information Act and Privacy Act Monitor or Records Manager determines if the information is releasable to the public, contains privacy act data, or is subject to the Reports Control System. The Records Manager may also update the web site OPR’s files plan to include the Internet Release Package, according to paragraph 7.5.

A5.1.4.5. Public affairs reviews publicly accessible web sites to ensure information made available to the general public follows criteria outlined within AFI 35-101, *Public Affairs Policies and Procedures*.

A5.1.5. Document approval by all reviewing officials. Return disapproved packages to the web site OPR with the reason for disapproval.

A5.1.6. The web site OPR maintains the approved Internet Release Package for the entire time the information resides on the publicly accessible web site, according to paragraph 7.5 of the basic instruction.

A5.1.7. When the web site is significantly revised, the web site OPR updates the original Internet Release Package and regains approval. Minor changes do not require reapproval.

A5.1.8. The web page OPR must review the web site quarterly to ensure unauthorized information has not been posted to the site and validate accuracy of the information. Use USAFE Form 884 to document quarterly reviews and file with the original Internet Release Package. If new information types are found on the web site, remove the information immediately until the web site is reapproved.

A5.2. Restricted Site Procedures. Follow guidance for public sites. Forward approved pages to local communications squadron for posting to base limited access server. The web site OPR maintains the approved Internet Release Package according to paragraph 7.5 in the basic instruction.

DAVID B. WARNER, Colonel, USAF
Director, Communications and Information