

**BY ORDER OF THE
SECRETARY OF THE AIR FORCE**

AIR FORCE INSTRUCTION 33-129

1 JANUARY 1997



**AIR MOBILITY COMMAND
Supplement 1**

11 MAY 1998

Communications and Information

**TRANSMISSION OF INFORMATION
VIA THE INTERNET**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the SAF/AAD WWW site at: <http://afpubs.hq.af.mil>. If you lack access, contact your Publishing Distribution Office (PDO).

OPR: HQ AFCA/RMI
(Lt Col Cynthia M. Mackey)

Certified by: HQ USAF/SCXX
(Col Brian D. Miller)
Pages: 34
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 37-1, *Air Force Information Management* (being converted to AFPD 33-3); AFPD 35-2, *Public Communications Programs*; AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*; and AFPD 33-2, *C4 Systems Security*. This instruction applies to all Air Force military and civilian personnel, including Air National Guard (ANG) and Air Force Reserve (AFRES), and their use of public internet and web technology such as web servers, web browsers, and file transfer protocol (FTP) software purchased and licensed by the United States Air Force (USAF), or privately licensed software used with proper approval on USAF-owned systems. This includes servers maintained by base communications personnel as well as servers maintained on small computers distributed throughout the Air Force. Failure to observe the prohibitions and mandatory provisions of this instruction as stated in **6.1.1.** through **6.1.12.** by military personnel is a violation of Article 92, Uniform Code of Military Justice (UCMJ). Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Direct questions or comments regarding the technical content of this instruction through appropriate major command (MAJCOM) channels to Headquarters Air Force Communications Agency, Information Resources Division (HQ AFCA/RMI), 203 West Losey Street, Room 1020, Scott AFB IL 62225-5233. Refer recommended changes and conflicts between this and other publications, using AF Form 847, **Recommendation for Change of Publication**, through channels, to HQ AFCA, Plans and Analysis Division, Policy Branch (XPPD), 203 West Losey Street, Room 1065, Scott AFB IL 62225-5224. MAJCOMs, field operating agencies (FOA), and direct reporting units (DRU) send one copy of their supplement to HQ AFCA/XPPD. Refer to **Attachment 1** for a glossary of references, abbreviations, acronyms, and terms.

(AMC) AFI 33-129, 1 January 1997, is supplemented as follows: (This supplement does not apply to the Air National Guard or U.S. Air Force Reserve units and members.) This supplement describes AMC

web publishing policy and responsibilities. This supplement contains guidelines and procedures for web page development and processing within AMC (reference AFI 33-115, *Network Management*, and AFI-33-112, *Computer Systems Management*).

SUMMARY OF REVISIONS

This is the initial publication of this AFI.

1.	Purpose.	3
2.	Appropriate Use of the Internet.	3
3.	Roles and Responsibilities:	3
4.	Web Administration.	7
5.	Requirements Processing.	10
6.	Access to the Internet.	10
7.	Clearing and Releasing Information Placed on the Web or Other Bulletin Boards. .	11
8.	Internet Pages:	13
9.	Single Source Information.	15
10.	Approval to Operate a Server on the Internet:	15
11.	System Security Considerations:	16
Table 1.	Security for Information Placed on the Internet/WWW.	19
Table 2.	Vulnerability of Information Placed on the Internet/WWW.	20
12.	Page Layout and Maintenance.	20
13.	Warning Notices and Banners.	21
14.	Registration of Uniform Resource Locators.	21
15.	Government Information Locator Service.	21
16.	Records Management.	22
17.	Electronic Mail.	22
Attachment 1—GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS		23
Attachment 2 (Added-AMC)—CHECKLIST FOR ESTABLISHING A WEB HOME PAGE		30
Attachment 3. (Added-AMC)—HOME PAGE APPROVAL PROCESS		32
Attachment 4. (Added-AMC)—AMC WORLD WIDE WEB RISK SUMMARY		33

1. Purpose. Use of the internet has dramatically increased in popularity as a means of obtaining and disseminating information worldwide. This instruction defines the roles and responsibilities of personnel using and maintaining internet access. It outlines responsibilities and procedures for accessing information and properly establishing, reviewing, posting, and maintaining government information on the internet. It also covers the responsibilities and procedures for sending e-mail across the internet. Guidance on the technical network access is covered in AFI 33-115, *Networks Management*. Failure to observe the prohibitions and mandatory provisions of this instruction in 6.1.1. through 6.1.12. by military personnel is a violation of Article 92, Uniform Code of Military Justice (UCMJ). Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal sanctions for violations of related laws.

2. Appropriate Use of the Internet. The internet provides opportunities for quick and efficient disseminating of information to the public, distributing information throughout the Air Force, and accessing information from a variety of sources. Information may be sent between offices or individuals, or be displayed on the web. The Air Force goal for the internet is to provide maximum availability at acceptable risk levels for Air Force members needing access for the execution of official business.

3. Roles and Responsibilities:

3.1. Headquarters United States Air Force, Deputy Chief of Staff/Communications and Information (HQ USAF/SC) will develop policy and guidance on using the internet.

3.2. Secretary of the Air Force, Office of Public Affairs (SAF/PA) will:

3.2.1. Develop policy and guidance for release of information to the public.

3.2.2. Provide and maintain Air ForceLINK, the official USAF World Wide Web (WWW) Home Page.

3.3. HQ USAF functional managers will determine the level of protection required when placing functional information on the internet or when sending it by e-mail.

3.4. MAJCOMs/FOAs/DRUs will:

3.4.1. Implement this instruction in their organizations.

3.4.2. Ensure all offices with e-mail establish an e-mail address according to AFI 33-127, *Electronic Messaging Registration and Authority*.

3.4.3. (Added-AMC) HQ AMC/PA (Office of Public Affairs) will:

3.4.3.1. (Added-AMC) Provide and maintain a MobilityLINK web site. The MobilityLINK is AMC/CC's public information web site, not a Public Affairs web site. MobilityLINK is the only authorized web source for public information. Any information to be released to the public (non .mil or not password protected) must be associated with MobilityLINK.

3.4.3.2. (Added-AMC) For the headquarters staff, the Director of Public Affairs is the only releasing authority for public information.

3.4.3.3. (Added-AMC) Provide assistance to Web Management Group (WMG), Directorate Web Supervisors and Web Page Maintainers in making information public.

3.4.4. (Added-AMC) Wing PA Offices will:

3.4.4.1. (Added-AMC) Provide and maintain a public web site for their respective location.

3.4.4.2. (Added-AMC) Approve clearance of information for public release on the web.

3.4.5. (Added-AMC) WMG will:

3.4.5.1. (Added-AMC) Provide assistance to directorates and wing level/web POCs on using the web as a resource.

3.4.5.2. (Added-AMC) Create and maintain documentation for web information to include:

3.4.5.2.1. (Added-AMC) An index of AMC web pages to the directorate/division level

3.4.5.2.2. (Added-AMC) Information approval (2-digit)

3.4.5.2.3. (Added-AMC) Directorate POC and alternate information

3.4.5.3. (Added-AMC) Periodically review subordinate and tenant web sites to ensure compliance with DoD, Air Force, AMC and local policies regarding links, accessibility, style and infrastructure.

3.4.5.4. (Added-AMC) Develop policies for correcting non-compliance. Furthermore, have authority for termination of pages/sites when OPRs cannot or will not comply.

3.4.5.5. (Added-AMC) Review information for release under the Freedom of Information Act and Privacy Act for the headquarters staff with the help of HQ AMC/SCYN (FOIA office).

3.4.5.6. (Added-AMC) Make recommendations to add or remove information for both public and internal release (e.g., information must have value to internal or external audiences). Specifically, no duplication of other Air Force sites information. Example: Delete local pages having promotion score data when Air Force Personnel Center (AFPC) has it posted the day line numbers are released. A link to AFPC sight is sufficient.

3.4.5.7. (Added-AMC) Responsible for maintaining top level (above 2-digit) pages of Air Mobility Command web site and AMC home page.

3.4.5.8. (Added-AMC) Direct customers to the appropriate office for infrastructure upgrades to meet mission needs.

3.4.5.9. (Added-AMC) Ensure POCs' requests for new components required to implement unique web requirements have:

3.4.5.9.1. (Added-AMC) Approved AF Form 3215, **C4 Systems Requirements Document (CSR)**

3.4.5.9.2. (Added-AMC) Written verification by Air Force Network Control Center (AFNCC) ensuring network infrastructure can support the requirement

3.4.5.9.3. (Added-AMC) End user issues have been addressed by POCs (e.g., availability of plug-ins, funding for software/hardware, etc.)

3.4.5.9.4. (Added-AMC) Technology available to the entire staff/command, not just a select few

3.4.6. (Added-AMC) Chief Information Officer (CIO) will:

3.4.6.1. (Added-AMC) Oversee command policies and guidance for making electronic information available on the web, both public and .mil restricted sites.

3.4.6.2. (Added-AMC) Keep abreast of current and emerging web technology.

3.4.7. (Added-AMC) Each Directorate Web Supervisor will:

3.4.7.1. (Added-AMC) Create and maintain an index of all directorate web pages.

3.4.7.2. (Added-AMC) Provide assistance to Directorate Web Page Maintainers on building, maintaining and updating directorate web pages and how to use the web as a resource.

3.4.7.3. (Added-AMC) Fund any components required to implement their unique web requirements. Funding will include end user cost if additional software/hardware is needed by all end users. Upon completion of approved CSRD (AF Form 3215), the WMG's and AFNCC's approval is needed to ensure network infrastructure can support the requirement. NOTE: The WMG and AFNCC may be the same office at base level.

3.4.7.4. (Added-AMC) The WMG depends on Directorate Web Supervisors to ensure information is current and correct. Directorate Web Supervisor must be chosen wisely to ensure continuity and corporate interest is represented. The director will designate both a primary and alternate Directorate Web Supervisor in writing to the AMC WMG. The primary Directorate Web Supervisor must be a DoD employee. Any changes of the Directorate Web Supervisor will require an updated letter of designation prior to activation of any individual as Directorate Web Supervisor.

3.4.7.5. (Added-AMC) Responsible for posting all directorates' related pages to the web server.

3.5. Air Force Educational Institutions will comply with Department of Defense Directive (DoDD) 5230.9, *Clearance of DoD Information for Public Release*, and AFI 35-205, *Air Force Security and Policy Review Program* ensuring that students and faculty are afforded the necessary latitude to conduct open scholarly/scientific collaboration.

3.6. Commanders and Supervisors will:

3.6.1. Ensure assigned personnel use government equipment for official or authorized use only.

3.6.2. Authorize only legal and ethical use of the internet that is in the best interest of the Air Force.

3.6.3. Authorize personal use of e-mail only when that use complies with all the stipulations below.

3.6.3.1. Does not interfere with the performance of official duties.

3.6.3.2. Is of reasonable duration and frequency.

3.6.3.3. Serves a legitimate Air Force interest such as notifying family of travel changes while on temporary duty (TDY), communications from place of duty required during duty hours, or morale purposes if stationed for an extended period away from home.

3.6.3.4. Creates no additional expense to the Air Force.

3.6.4. Obtain all internet access through the supporting C4 systems officer (CSO).

3.7. CSO will:

- 3.7.1. Efficiently manage base internet facilities to ensure only authorized equipment and software necessary to perform official government business is procured and maintained.
- 3.7.2. Ensure internet connectivity is monitored and controlled by the base network control center (BNCC).
- 3.7.3. Advertise this instruction to users of the internet.

3.8. BNCC will:

- 3.8.1. Control all internet connections, to include military controlled access paths and alternate internet access paths, such as Internet Service Providers (ISP).
- 3.8.2. Ensure all traffic destined for other military sites (within the ".mil" domain) is only routed through military controlled networks (that is, traffic destined for military sites will not be routed through an ISP and traffic from an ISP will not be routed through the receiving base network to other military networks).
- 3.8.3. Ensure "af.mil" network domains are not advertised through ISP connections. *Note: Only the Air Force Network Support Center, Gunter AFB AL is authorized to establish connections to the "af.mil" network domain.*
- 3.8.4. Ensure access to the internet is secured to acceptable risk levels as defined in [11](#).

3.8.5. (Added-AMC) Wing SC (AFNCC) units will:

- 3.8.5.1. (Added-AMC)** Ensure that all base web servers are properly accredited and the OPRs are aware of their computer security responsibilities according to this instruction.
- 3.8.5.2. (Added-AMC)** Provide users with technical solutions to web browser access and home page implementation. Each OPR will use [Attachment 4. \(AddedAMC\)](#) as a guidepost for their security acquisition strategy and should reference Air Force Systems Security Memorandum (AFSSM) 5018, *Risk Analysis*, and AFSSM 5022, *Network Risk Analysis Guide*.
- 3.8.5.3. (Added-AMC)** Base Records Management Office will review information for wing-level staff for release under the Freedom of Information Act and Privacy Act.
- 3.8.5.4. (Added-AMC)** Fund any components required to implement unique web requirements. Funding will include end user cost if additional software/hardware is needed by all end users. Upon completion of an approved CSRD (AF Form 3215), the WMG's and AFNCC's approval is needed to ensure network infrastructure can support the requirement.

3.9. C4 Systems Security Officer (CSSO). Where dial-up access is absolutely necessary, will notify supporting BNCC of the intent to use dial-up subscription services and ensure computers used for such access do not have an active network routing capability and are protected by the most current available virus protection.

3.10. Users will:

- 3.10.1. Use government equipment and access the internet only for official business or authorized activities.
- 3.10.2. Determine the sensitivity and apply appropriate protection to all information transmitted using the internet.

- 3.10.3. Adhere to copyright restrictions.
- 3.10.4. Protect passwords and access codes.
- 3.10.5. Ensure that all official records created while using the internet are placed in the official record management system (see AFI 37-122, *Air Force Records Management Program*).
- 3.11. Information Provider. Provides material (for example, text, graphics, and so forth) to the page maintainer for posting on the web. The information provider is the point of contact (POC) of the material's subject matter and is responsible for:
 - 3.11.1. Ensuring material is reviewed by the appropriate office according to USAF policies, and identifying security and access controls required before it is posted on the internet.
 - 3.11.2. Ensuring material is properly cleared and documented for release on the internet by the releasing authority (see AFI 35-205 for release procedures and authority).
 - 3.11.3. Validating the accuracy of all material provided to the page maintainer.
 - 3.11.4. Ensuring outdated or superseded information is identified and promptly removed from the system.

4. Web Administration.

- 4.1. Web Server Administrator. The top-level home page for each web server will have a web server administrator identified by name, office symbol, phone number, and e-mail address. This individual is the POC for customers having problems with web documents on that server.
 - 4.1.1. The web server administrator is responsible for:
 - 4.1.1.1. Maintaining the server's top-level home page.
 - 4.1.1.2. Operation of the server.
 - 4.1.1.3. Security of the server.
 - 4.1.1.4. Maintaining access and security control features.
 - 4.1.1.5. Ensuring designated approving authority (DAA) approval is reaccomplished if any configuration changes are made to the system.
 - 4.1.1.6. Registering site with *Air ForceLINK*.
 - 4.1.1.6. (AMC)** AFNCC Web Management Office is the authorized POC for registering their sites with Air ForceLink. Directorate Web Supervisor/Page maintainers wishing to register their site with Air ForceLink will forward their requests through the AFNCC Web Management Office.
 - 4.1.1.7. Ensuring all links from pages under their control are appropriate and valid.
 - 4.1.1.8. Establishing procedures for page maintainers to place information on the web server.
 - 4.1.1.9. Granting and monitoring write-access privileges.
 - 4.1.1.10. Maintaining and evaluating audit control logs.
 - 4.1.1.11. Gathering and analyzing performance data on servers under their control.
 - 4.1.1.12. Developing, coordinating, publishing, maintaining, and testing support plans for

contingency and service restoration.

4.1.1.13. Coordinating mirror or replication sites with other system administrators.

4.1.1.14. Implementing security and access controls requested by page maintainers.

4.2. Page Maintainer. Each subordinate page under the top-level home page will have a POC identified for information on that page. Page maintainers are members of the organization having overall responsibility for the page's subject matter. They develop and maintain the actual information file and are responsible for ensuring both the page content and presentation is consistent with Air Force policy. Page maintainers assist the web server administrator with implementing the appropriate access and security controls to protect the information resource.

4.2.1. Each page maintainer is responsible for:

4.2.1.1. Developing and maintaining subordinate-level pages.

4.2.1.2. Reviewing, documenting, and obtaining release authority on material before posting it to the page.

4.2.1.3. Validating all links from pages under their control.

4.2.1.4. Ensuring proper access and security controls are in place and operational.

4.2.1.5. Maintaining access lists.

4.2.1.6. Ensuring user identifications (ID) and passwords are in compliance with Air Force and local security policy, and are current.

4.2.1.6. (AMC) Passwords should be a random combination of alphanumeric characters. Users will change their passwords every 90 days. The Web Management Office will remove accounts found inactive for 90 days or longer. Accounts that have not had a password change in over 90 days will also be removed. IMAs should get with their Work Group Manager (WGM) for special user ID and password.

4.2.1.7. Ensuring outdated or superseded information is removed from the system.

4.2.1.7. (AMC) Information placed on any web server will, as a minimum, be reviewed quarterly to ensure currency. The appropriate page maintainer will document quarterly reviews.

4.2.1.8. Incorporating a feedback mechanism for users' comments.

4.2.1.8. (AMC) Feedback mechanisms can range from a "mailto" link to Common Gateway Interface (CGI) script files and forms.

4.2.2. (Added-AMC) Each Web Page Maintainer will:

4.2.2.1. (Added-AMC) Identify web requirements through appropriate channels and obtain approval in accordance with AMC and local policies.

4.2.2.2. (Added-AMC) Fund any components required to implement their unique web requirements. Funding will include end user cost if additional software/hardware is needed by all end users. Upon completion of approved CSR (AF Form 3215), the WMG's and AFNCC's approval is needed to ensure that network infrastructure can support the requirement.

4.2.2.3. (Added-AMC) As information OPRs, screen their information to determine its value and the security risk associated with making the information available on the web. Information owners will ensure appropriate access and security controls are implemented and used.

4.2.2.4. (Added-AMC) Develop and maintain the currency of information on their respective sites. Information will be reviewed for accuracy at least every 30 days.

4.2.2.5. (Added-AMC) Create user IDs and passwords as required for users to access limited release information.

4.2.2.5.1. (Added-AMC) Ensure user IDs and passwords are kept current. Ensure passwords are changed every 90 days. Delete user IDs and passwords when users PCS, retire or separate.

4.2.2.5.2. (Added-AMC) Develop procedures for users to obtain access to password protected areas. Procedures should be easily accessible on non-restricted web area.

4.2.2.6. (Added-AMC) Ensure the Directorate Web Supervisor completes testing of new or modified web pages prior to placement onto the web site.

4.2.2.7. (Added-AMC) Ensure the Directorate Web Supervisor completes a review of updated pages after placement on the web to ensure the information transfer was accomplished accurately.

4.2.2.8. (Added-AMC) Coordinate with their directorate on web page content.

4.2.2.9. (Added-AMC) Coordinate project-related information through the appropriate manager prior to placement on the web.

4.2.2.10. (Added-AMC) Maintain working knowledge of current HTML design standards.

4.2.2.11. (Added-AMC) Submit all *.mil* (private) URL information to AMC WMG for indexing and public URL information to HQ AMC Public Affairs Office for referencing on public pages.

4.2.2.12. (Added-AMC) Ensure each public home page has an accompanying Government Information Locator Service (GILS) record. The purpose of GILS is to provide a convenient, organized system for the public to access Federal Information Resources. The Air Force point of entry into GILS is Air ForceLINK and its associated public access pages. All public access pages are required to develop an associated GILS Core Records. Office of Management and Budget (OMB) Bulletin 95-01 describes GILS and the data elements required for the GILS Core Records. All Public Dissemination Products (PDP), regardless of media, must have an associated GILS Core Record posted to Air ForceLINK. PDPs are information products produced by the Air Force specifically for the public. PDPs do not have to be converted to an electronic media and placed on Air ForceLINK; however, the GILS Core Record must reflect where to gain access to the PDP.

5. Requirements Processing. Follow AFI 33-103, *Requirements Development and Processing*, when submitting requirements for internet access, the need to place information on a web server, view information on the WWW, develop information to place on a web page, or obtain e-mail capability. The CSO develops technical solutions based on the entire base C4 infrastructure and internet needs. CSOs will

limit the number of servers to the minimum number needed to distribute the information. One server may serve many different users and organizations.

6. Access to the Internet.

6.1. Accessing the internet through a government computer or network uses a government resource. Government-provided hardware and software are for conducting official and authorized government business. This does not prohibit commanders from authorizing personnel to use government resources to further their professional and military knowledge if they determine it is in the best interest of the government and authorization is documented by letter, local operating instruction, or explicit policy. Using the internet for other than authorized purposes may result in adverse administrative or disciplinary action. The following activities involving the use of government-provided computer hardware or software listed in 6.1.1. through 6.1.12. are specifically prohibited:

6.1.1. Any use of government-provided computer hardware or software for other than official and authorized government business.

6.1.2. Activities for personal or commercial financial gain. This includes, but is not limited to, chain letters, commercial solicitation, and sales of personal property.

6.1.3. Storing, processing, displaying, sending, or otherwise transmitting offensive or obscene language or material. Offensive material includes, but is not limited to, "hate literature," such as racist literature, materials or symbols (for example, swastikas, neo-Nazi materials, and so forth), and sexually harassing materials. Obscene material includes, but is not limited to, pornography and other sexually explicit materials.

6.1.4. Storing or processing classified information on any system not approved for classified processing.

6.1.5. Storing or processing copyrighted material (including cartoons) unless approval is obtained from the author or publisher.

6.1.6. Participating in "chat lines" or open forum discussion unless for official purposes and after approval by appropriate Public Affairs channels.

6.1.7. Using another person's account or identity without appropriate authorization or permission.

6.1.8. Viewing, changing, damaging, deleting, or blocking access to another user's files or communications without appropriate authorization or permission.

6.1.9. Attempting to circumvent or defeat security or auditing systems without prior authorization or permission (such as for legitimate system testing or security research).

6.1.10. Obtaining, installing, copying, storing, or using software in violation of the appropriate vendor's license agreement.

6.1.11. Permitting any unauthorized individual access to a government-owned or government-operated system.

6.1.12. Modifying or altering the network operating system or system configuration without first obtaining permission from the administrator of that system.

6.2. Each Air Force base and deployed force package network will have a single, logical point of internet access provided and defended by the BNCC.

6.3. Dial-Up Internet Services. Dial-up access to internet service providers, such as *America On Line*, *CompuServe*, or others, is prohibited for users with internet access through base and deployed networks, except when an organizational subscription is established for official business and the account is specifically authorized by the unit commander (see 3.8. and 5. for requirements identification and processing procedures).

6.4. Non-Mission Related Internet Services. As stated in 3.7., the BNCC is responsible for controlling all internet access. For security reasons, devices that provide public access to the internet for non-mission related activities (typically located in the library or morale, welfare, and recreation [MWR] facilities) shall not be connected to the base network with the privileges of "af.mil" registered users. Only mission related activities shall be registered "af.mil" users. The BNCC may establish common access for non-mission related users provided these users are not allowed unauthorized access to base, Air Force, or government resources.

7. Clearing and Releasing Information Placed on the Web or Other Bulletin Boards.

7. (AMC) The release authority for .mil domain will be the 2-digit head/designated representative or commander of the organization releasing the information.

7.1. Office of Primary Responsibility (OPR). The OPR is the creator and/or focal point for specific material posted on the organizational home page. The OPR is responsible and accountable for protecting its information resource and ensuring the requirements for release of information are satisfied. The OPR must also determine which functional areas need to review the material and identify any risks associated with the release of information. Information released to the internet may only be done by, or with the written consent of the OPR.

7.2. Public Access. Each OPR should recognize that "public access information" refers to that information approved for "unlimited" access and distribution on the internet. The various types of information are cleared for release the same way as hard copy information is cleared. Public access information has no access or security controls to limit access to the information. According to AFI 35-205, the public affairs office (PA) will provide security and policy review at the OPR's request. This review determines the degree of releasability only; actual release of the material is the decision of the release authority (normally the senior organization or installation commander or their designee).

7.2.1. Procedures for Clearing Information for Public Access.

7.2.1.1. Since the intended audience for public access information is the general public, no access or security controls are necessary. However, servers must ensure public access cannot contaminate Air Force pages or gain access to other parts of the Air Force system. Use the same process taken to release information in paper form to review information prior to release on the WWW.

Table 1. identifies some of the directives or instructions applicable to any review of information for public release. Do not regard **Table 1.** as the sole source for identifying reviewing authorities. You may find additional guidance on the releasability of information with the PA, foreign disclosure office, the scientific and technical information (STINFO) officer, the *Security Classification Guide*, and the *Operations Security (OPSEC) Guide*.

7.2.1.2. When reviewing information for public release, remember that the information should be of value to the general public. Do not place information that has value to only mili-

tary or other government agencies on internet pages with unlimited access.

7.3. Limited Access. Each OPR should recognize that "limited access information" refers to that information released on the internet with restrictions on file or data base access appropriate for the type of information involved. This information has added safeguards that limit the access to specific individuals or groups. The OPR must determine the appropriate security and access controls required to safeguard the information (see [Table 2](#)).

7.3.1. Procedures for Clearing Information for Limited Access. The same channels taken to release information in paper form is used to screen information for limited access. Since the internet provides access across a number of interconnected networks, information without access controls on a server directly connected to the internet is potentially available to anyone on the internet. When information is cleared for limited access, access controls and/or encryption is necessary to protect the information. Remember, the intended audience will vary depending upon the information and its potential intelligence value. Also remember that unclassified information when combined with other available information, may become sensitive or even classified. This presents a significant threat to the information resource. Where appropriate, refer to the *Security Classification Guide* or contact the OPSEC office or base information protect office for assistance. When in doubt, take the extra time--check it out.

7.3.1.1. To place information on the internet, the OPR must stay aware of the types of security and access controls possible and the vulnerabilities of each. [Table 2](#) outlines generic security and access controls for the internet with the recommended employment of each. Also, use [Table 2](#) as a guide to determine the acceptable risk for releasing information. If the network is a non-public network (that is, an internal local area network [LAN] or base-wide metropolitan area network [MAN]), the physical layout of the network may already provide a certain level of access control that should be taken into consideration when determining acceptable risk.

7.4. Information Not Appropriate for Public Release. Under no circumstances will the following types of information be placed on web sites that are available to the general public. OPRs placing this information on limited access sites are responsible for meeting all DoD and Air Force requirements for safeguarding information:

7.4.1. Classified information (see AFI 31-401, *Managing the Information Security Program*).

7.4.2. Privacy Act protected information (see AFI 37-132).

7.4.3. For Official Use Only (FOUO) information (see AFI 37-131).

7.4.4. DoD contractor proprietary information (see AFI 61-204).

7.4.5. STINFO (see AFI 61-204).

7.4.6. Unclassified information requiring special handling (see AFI 33-113, *Telecommunications Centers and Data Processing Centers Management*).

7.4.7. Critical information as outlined in AFI 10-1101, *Operations Security (OPSEC) Instructions*. Sensitive mission data that by itself is unclassified, but when combined with other available data, may reveal classified information.

7.4.8. Freedom of Information Action (FOIA) exempt information for which the agency declines to make a discretionary disclosure (see AFI 37-131).

7.5. Document the Process. Prior to release, OPRs will coordinate and document the process used to review information destined for internet release. Review processes may vary depending on the type and value of the information you are considering releasing (that is, releasability of standard publications is determined prior to publication; a blanket review and clearance for unclassified standard publications are sufficient). Maintain completed "Internet Release Packages" in the OPR's official files until the corresponding information is removed from the internet. Maintain these files according to the office file plan and Air Force Manual (AFMAN) 37-139, *Records Disposition Schedule*, Table 37-18, Rule 17. The OPR is accountable in the event of unauthorized disclosure of limited access information.

7.5. (AMC) Use checklist at **Attachment 2 (AddedAMC)** to develop a "Checklist for Establishing a Web Home Page." **Attachment 3. (AddedAMC)** provides an example of a "Home Page Approval Process" and **Attachment 4. (AddedAMC)** gives you the "AMC World Wide Web Risk Summary" information.

8. Internet Pages: A "page" is a document, including the text of the document, its structure, any links to other documents, images, and other media provided to a web browser in response to a request. A "home page" is the screen or page designed by an organization as its front page.

8.1. Types of Pages:

8.1.1. Public Access Pages (Organizational). Public access pages are intended for viewing by the general public, and the information that goes on these pages should be of interest to the general public. Information that would not be of interest to the general public should not be on a public access page. Universal source locator addresses should follow the standard protocol used throughout the web. For instance, a site representing all of Dover Air Force Base to the public would most logically be located at <http://www.dover.af.mil>. Bases/MAJCOMs should have only one official home page for the base that serves as the virtual "visitor's center" for that base/MAJCOM. The base PA will coordinate on the content and layout of the base's home page. Register the Uniform Resource Locator (URL) or "address" for the base home page with *Air ForceLINK* the "official" installation home page (see [14.](#)). Use a separate server or partition to prevent access to restricted information by non-Air Force personnel.

8.1.2. Limited Access Pages (Organizational). Limited access pages are intended for viewing by a limited audience. The audience for this information varies with the type of information. Air Force organizations that intend to use internet and web technology for distribution of information within the Air Force should develop an intranet or limited access pages rather than use public access pages on the WWW. An intranet is a limited access network that uses web technology but is not directly connected to the public internet. Information approved for limited release must have added safeguards and security controls to limit access by other internet users. Restrict pages and bulletin boards to selected users by accepting connects from internet protocol (IP) addresses ending in ".mil" or ".gov" and/or by requiring a password. (See [Table 1.](#) and [Table 2.](#) for minimum access/security control required for information types.)

8.1.3. Individual Pages. Develop individual pages only if a page is suitable for a specific duty position. For example, an individual page may be appropriate for an organizational commander or director but is not appropriate for a flight or branch chief. Personal pages are normally inappropriate; the rare exception being for specifically approved functions such as educational purposes. Under no circumstance should the page extend beyond the official duties and position of the indi-

vidual. Listing hobbies, favorite vacation sites, family photos, resumes, and preferred web sites is not appropriate.

8.2. Page Components.

8.2.1. Hypertext References or Pointers.

8.2.1. (AMC) Commercial links are strictly prohibited on public accessible web servers. In addition, specifying which browser works best on a particular web page could be taken as advertising. There will be no links or mention of specific web browsers on any web pages. Web pages should be created to take advantage of the most commonly used browsers. Creating a web page to take advantage of one particular web browser is prohibited.

8.2.1.1. Refrain from having pointers on public access pages that reference information that is outside the mission or functional area of the OPR. In most cases, home pages should refer or point only to parent commands and/or subordinate units. Installation home pages should provide pointers to base organizations as well as to the MAJCOM-level home page. Similarly, organizational home pages should have pointers up and down the chain of command. All pages designed to provide public access information should refrain from referencing limited access areas. Pointers to commercial organizations or associations are inappropriate as some may construe them as advertisements or endorsements.

8.2.1.1. (AMC) There will be no links or references to commercial and restricted access sites on the publicly accessible web servers.

8.2.1.2. Restrictions on pointers for limited access pages are not as stringent as those for public access pages. Pointers may point to a variety of military, government, educational, and organizational pages that provide information for use in the performance of official duties. Pointers may point to commercial organizations only if the information is necessary to the performance of official duties.

8.2.1.2. (AMC) There will be no links to commercial organizations on limited access pages, unless it can be proven beyond a shadow of doubt that the link pertains to the subject matter on the page containing the link. Links to commercial search engines and counter sites are prohibited.

8.2.2. Meta-Indexes, Indexes, or Lists of Other Air Force and DoD Pages. Indexes and lists will only reside on MAJCOM and at *Air Force Link*, the Air Force's service-level site. Local pages should refer to these centralized lists. Additions, deletions, and changes to the Air Force index are sent via e-mail to the address listed on *Air ForceLINK*. MAJCOMs will extract their portion of the list from the *Air ForceLINK* index. Indexes and lists are limited to those sites that provide relevant information to the intended audience.

8.2.3. Phone Numbers and Electronic Mail Addresses. Placing directories of all telephone and electronic mail addresses on public pages is prohibited. Providing such addresses invites mass mailings by commercial agencies and exposes organizations to attempts to overwhelm or "Spam" local networks with thousands of simultaneous and unwanted electronic mail messages. This does not prevent organizations from putting this information on intranet, or internal web sites, using limited domain or other restrictions. In addition, public pages are encouraged to "publish" general numbers of services such as the base locator, public affairs, and other commonly requested resources.

8.2.4. Advertising. Commercial advertising and product endorsement on Air Force web sites are prohibited.

8.2.5. Use of Graphics and Artwork. Great care must be taken when adapting existing artwork for use on internet projects. For instance, most licenses for software designed to prepare documents or briefings do not permit the user to use the graphics for other purposes. In addition, most artwork is either copyrighted or proprietary and will not be used unless permission is gained from the originator in writing. Consultation with local legal staffs is essential.

8.2.6. (Added-AMC) All locally approved icons, backgrounds and graphics will be maintained in an on-line library by each base Visual Information (VI) center and referred to as a clip-art library. In addition, the Scott AFB VI center will maintain a library of command level graphics, i.e., the AMC shield. Base library pages should display command graphics as well as local graphics. The command graphics do not have to reside on that base's web server. Example, McConnell AFB VI center library pages may have an AMC shield but it will be linked to the shield on the Scott AFB VI server. This ensures if a change is made all bases have access to the approved command graphics.

8.2.7. (Added-AMC) Base VI Center will also coordinate on the layout of base's home page. All home pages should be reviewed by VI for composition, graphic format and viewability.

9. Single Source Information. Information should remain as closely controlled by the source as possible to ensure its currency and accuracy. Do not copy files from other sources on the internet and place them on a home page. Reference this information rather than repeat it. This does not prevent information providers from mirroring or replicating information for performance or security reasons. However, when this is done, the information provider of the replicating file server should contact the OPR of the information to get written permission to replicate the information and must establish procedures for updating the information. In addition, the page manager or web server administrator must verify the releasability of the information.

10. Approval to Operate a Server on the Internet:

10.1. DAA Approval. According to DoD Directive (DoDD) 5200.28, *Security Requirements for Automated Information Systems (AISs)*; Air Force Systems Security Memorandum (AFSSM) 5003, *Designated Approving Authority Guide*; and AFD 33-2, all systems must receive accreditation and authorization to operate by the appropriate DAA prior to actual use. This applies to all servers directly connected to the internet. You must perform a network risk analysis along with a network security plan (see AFSSM 5022, *Network Risk Analysis Guide*, for directions in preparing a network risk analysis). Determine the appropriate level of security from the risk analysis. DAA approval is reaccomplished anytime there is a significant change in sensitivity of information provided on the server (that is, server initially accredited for public access information that now contains limited access information). Failure to reaccredit will result in disconnection.

10.2. Auditing of User Activity. Configure systems so that the system administrator can audit both incoming and outgoing user activities. Auditing of incoming user activities helps identify possible security threats as well as provide OPRs feedback on the usefulness of their information. Auditing of outgoing user activity helps ensure government systems are not misused. Organizations can keep misuse of computer systems to a minimum by training and educating personnel on proper uses of the internet and monitoring their activity. (Monitoring of communications circuits alone will not prevent

misuse.) Filter all internet requests through a "proxy server" in order to effectively monitor outgoing and incoming activities.

11. System Security Considerations:

11.1. Internet Vulnerabilities. Because the internet is a public network, information placed on the internet without access controls is available to everyone. Using access controls effectively reduces the risk of accessing information on the internet.

11.1.1. Internet Controls. Restricting access to information is only part of the security equation. The internet is an inherently unsecured network. Information packets traveling across the internet jump from node to node to travel from origin to destination. At any point along the way, interception of the information can occur. To prevent unauthorized disclosure of information, security controls must be implemented. Any security controls implemented in the internet must meet Federal Information Processing Standard (FIPS) 140-1, *Security Requirements for Cryptographic Modules*. Therefore, to fully protect information resources, it takes a combination of access and security controls.

11.1.2. Internet Threats--Structured and Unstructured Attacks. Internet access growth, coupled with the increase of information stored, processed, or transmitted on Air Force computer systems increase the threat and vulnerability of Air Force information resources. Network attacks from the internet primarily come in two forms--structured and unstructured.

11.1.2.1. Structured attacks are sophisticated and organized, and are the most severe threat to our systems and our information resource. Structured attacks come from groups of individuals who have common goals. These groups target specific systems or groups of systems for industrial and military espionage, malicious intentions, financial gains, and, or military operational advantage.

11.1.2.2. Unstructured attacks are less organized but usually employ the same techniques as structured attacks. For example, the common computer "hacker" is an unstructured attacker. These attackers pick their targets at random, probing different domains in search of common system vulnerabilities to exploit. Individual attackers infiltrate systems out of curiosity to boast their success in the hacker community, enabling them to achieve a higher status. They may, however, have malicious intentions (for example, implanting logic bombs, Trojan horses, denial of service attacks, or altering data) just to cause grief to the system's legitimate users.

11.1.2.3. Countering the Threat. The Air Force has implemented a robust program to thwart most of these threats through a program called "Information Protection." The Air Force Information Warfare Center (AFIWC) is the Air Force's leader in identifying the threats and confronting attacks to our automated information systems. AFIWC works closely with the MAJCOM/base/wing information protection office. The local information protection office provides expertise in educating systems administrators, information providers, and page OPRs on current threats, vulnerabilities, and protection techniques. The skill and knowledge levels of the systems administrator, in concert with the applied technical solutions or "patches" available, are the key determinants in keeping a system and its information secure. In a web environment, the information providers are also key because they identify the value of the information and the type of access controls and techniques necessary to protect information from unauthorized disclosure. Systems administrators, information providers, and page OPRs

must maintain a close working relationship with the information protection office to remain aware of the ever changing threat to information and systems, and to report any unusual activity on a system. Listed below are some of the common techniques used to attack a system or its information:

11.1.2.3.1. IP Spoofing. Potential intruders attempt to gain access to a system or its information by creating packets with spoofed (faked) source IP addresses.

This exploits applications that use authentication-based IP addresses and leads to unauthorized user access, and possibly "root access" (the ability to control an entire computer system, even to the exclusion of the system owner). A seasoned systems administrator can thwart these techniques with information and software from the information protection office.

11.1.2.3.2. Packet Sniffers. Information traverses the internet in packets through a series of computers. These computers (routers, bridges) reside at any given point on the internet, and are most likely outside of DoD control. These computers are also vulnerable to the same computer threats as DoD systems, and an intruder may compromise them by gaining root access. Once an intruder has gained access, they can activate a program (such as a Trojan horse) to collect information traversing the computer (for example, internet domain, account names, IDs, and passwords). Generally, good password administration and encryption techniques can thwart this threat.

11.1.2.3.3. Trojan Horse. These are hidden computer viruses or viruses in disguise. Trojan horses are often computer programs embedded in other programs or software. This is done by the intruder so the user is unaware of the Trojan horse's presence or existence. Trojan horse programs do something the programmer intended but that the user would not approve of if they knew about it. A virus is a particular case of a Trojan horse that is able to spread to other programs. Some Trojan horses hide in a system and capture information (for example, IDs and passwords of legitimate users) so the programmer can return to the system at a later time to damage, destroy, or steal data. In the case of an ID/password capture or compromise, an intruder gains the capability of entering the system as a legitimate user.

11.1.2.3.4. Network Monitoring Attacks. Systems at risk are systems that offer remote access through remote login, TELNET, and FTP. This threat involves a monitoring tool that uses a promiscuous mode of a specific network interface to capture host and user authentication information on all newly opened FTP, TELNET, and remote sessions. Intruders typically install Trojan horse programs to support subsequent access to the compromised system and to hide their network monitoring process. This technique threatens all user account and password information derived from FTP, TELNET, and remote sessions passing through the same network as the compromised system.

11.1.3. Downloading Files from the Internet. To protect against downloading viruses, users must virus-check all downloaded files. This applies to sound and video files as well as files attached to e-mail messages. If possible, download files to a floppy disk and virus-check them before placing them on the computer's hard drive. If files are compressed, perform a second check of the decompressed files. To prevent the possibility of rapidly spreading a virus, do not download files to a network or shared drive. The Air Force allows the use of public domain or shareware software

only after it is certified by a software testing facility. Such as the AFIWC at Kelly AFB TX, the Software Technology Support Center at Hill AFB UT, or the Standard Systems Group at Maxwell AFB-Gunter Annex AL (see AFI 33-114, *Software Management*).

11.1.4. User IDs and Passwords. The use of passwords on Air Force systems is governed by Air Force Systems Security Instruction (AFSSI) 5013, *Password Management* (to be replaced by Air Force Manual [AFMAN] 33-223).

11.1.5. IDs and Password Protection. The internet is an unsecured network where compromise of a user ID and password can occur during open transmission. Do not transmit user IDs and passwords without encryption. Secure sockets layer (SSL) protocol provides a transmission level of encryption between the client and server machines. In addition to encryption protections for passwords, use one time password systems to ensure password integrity.

11.1.6. Access and Security Controls on Information. **Table 2.** provides guidance on access and security controls, and the vulnerability of various combinations of each. Use **Table 2.** in conjunction with **Table 1.** to help determine an acceptable level of risk for information release. Do not regard these tables as the sole source for this information.

11.1.7. OPSEC. The internet access available to personnel at home and at work is an additional security factor. OPSEC training and education apply to computer use just as it does in conversations between personnel, correspondence, and telephone conversations. Policies against communicating with unauthorized personnel also apply to internet communications. News groups (Network News Transfer Protocol [NNTP], Usenet News, Chats, etc.) give personnel the opportunity to converse electronically to a worldwide audience. Military and government employees should refrain from discussing work-related issues in such open forums. Such discussions could result in unauthorized disclosure of military information to foreign individuals, governments, or intelligence agencies or the disclosure of potential acquisition sensitive information. For example, news media monitoring the internet may construe an individual's "chat" as an official statement or news release.

Table 1. Security for Information Placed on the Internet/WWW.

TYPE OF INFORMATION	GOVERNING PUBLICATIONS	REVIEW PROCESS INCLUDES	MINIMUM ACCESS/SECURITY CONTROL
Public Access	AFI 35-205 AFI 35-206	Public Affairs (PA)	Unlimited/Unencrypted
Limited Access (see Note 1)	AFI 35-205 AFI 35-206 & other sources as required	Public Affairs (PA)	.mil & .gov/Unencrypted
Marked For Official Use Only (FOUO) (see Note 2)	AFI 37-131, paragraph 26	FOIA Manager	Password and ID
Privacy Act	AFI 37-132	Privacy Act Officer	Password and ID
DoD Contractor Proprietary Information	AFI 61-204	Contracting and Contractor's Written Consent	Password and ID
Freedom of Information Act (FOIA)-Exempt Information	AFI 37-131	FOIA Manager	Password and ID
Unclassified Scientific and Technical Information (STINFO) AFI 61-204			
Distribution Statement A	AFPD 61-2 AFI 61-204	STINFO Officer Public Affairs (PA)	Unlimited/Unencrypted
Distribution Statement B	AFPD 61-2 AFI 61-204	STINFO Officer	Password & ID/Encrypted
Distribution Statement C	AFPD 61-2 AFI 61-204	STINFO Officer	Password & ID/Encrypted
Distribution Statement D	AFPD 61-2 AFI 61-204	STINFO Officer	Password & ID/Encrypted
Distribution Statement E	AFPD 61-2 AFI 61-204	STINFO Officer	Password & ID/Encrypted
Distribution Statement F	AFPD 61-2 AFI 61-204	STINFO Officer	Password & ID/Encrypted

NOTES:

1. Certain types of information, though unclassified, may still have restrictions of foreign access. If this possibility exists, consult your local Foreign Disclosure Office for assistance. When the possibility of information becoming sensitive when aggregated with other non-sensitive information exists, the OPRs should consult the *Security Classification Guide* and, or operations security officer for assistance.

2. Must meet the criteria for exemptions 2 through 9 under AFI 37-131, paragraph 10.

Table 2. Vulnerability of Information Placed on the Internet/WWW.

If Access Control is:	and Security Control is:	the Vulnerability is:	and the Web Documents Should be those that are:
Unlimited	Unencrypted	EXTREMELY HIGH--open to everyone on the internet worldwide.	Publicly accessible, including STINFO -marked Distribution A.
Limited by Internet Domain (e.g., .mil, .gov) or IP Address	Unencrypted	HIGH--Can spoof access controls; affords the lowest level of access control; and no encryption.	Non-Sensitive; normally publicly accessible; OPR prefers material remain outside of public view.
Limited Access by User ID and Password	Unencrypted	MODERATE--Can spoof access controls; affords the highest level of access control, however, can compromise user IDs and passwords, since encryption is not used.	Non-Sensitive. Limited to small groups; OPR prefers protection of material with higher confidence of security.
Limited Access by Domain or IP Address	Encrypted	LOW--Provides encryption and the lowest level of access control.	Sensitive. OPR prefers material protected with high confidence of security.
Limited Access by User ID and Password	Encrypted	EXTREMELY LOW--Encryption with the highest level of access control.	Sensitive. Privacy Act, FOUO; DoD Contractor Proprietary, and STINFO with Distribution B-F.

12. Page Layout and Maintenance. You must ensure internet pages are professionally presented, current, accurate, factual, and related to the organizational mission. Use images appropriate to the content; do not use images indiscriminately. Do not display indicators to incomplete paths or use the phrase "under construction"; do not introduce information or services until they are ready. Announce new, or substantially changed information on the home page. Every internet page will contain the following information as a minimum:

12. (AMC) OPR information is critical to identify responsible individuals if there is a problem with a particular web page. All home pages will have the following information:

12.1. Page OPR name.

12.1. (AMC) Full name, rank or grade (if applicable)

12.2. Organization, office symbol, commercial phone number, and Defense Switched Network (DSN) phone number.

12.3. E-mail address.

12.4. Any disclaimers or restrictions that apply to the contents of the page.

12.5. (Added-AMC) Alternate point of contact.

13. Warning Notices and Banners. Present warning notices and banners on each home page. Tailor these warning notices and banners to the audience and types of information presented. If the type of information and audience changes, you should also change the warning notice and banners.

13. (AMC) Warning notices and banners will be placed prominently at the top of the home page (*or a JavaScript pop-up window will be adequate*). A link for individuals to click to read warning notices is not allowed.

13.1. Public Pages. Public pages will have the following warning notice and banner presented: "This Government Computer System is provided as a public service by the (name of the organization and Air Force base). It is intended for use by the public for viewing and retrieving information only. Unauthorized attempts to upload information or change information on this service are strictly prohibited and are punishable under the Computer Fraud and Abuse Act of 1986. Unless otherwise indicated, all information on this system is public information and is available to copy or distribute."

13.2. Limited Pages. Limited-access information that is covered by AFI 61-204 must use the warning notices identified in AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*. Place the warning notice at the beginning of the document, announcing the precise distribution statement. If the information is not covered by AFI 33-219, *Telecommunications Monitoring and Assessment Program (TMAP)*, use the following as a default warning notice and banner: "Official U.S. Government system for authorized use only. Do not discuss, enter, transfer, process, or transmit classified/sensitive national security information of greater sensitivity than that for which this system is authorized. Use of this system constitutes consent to security testing and monitoring. Unauthorized use could result in criminal prosecution."

13.3. Educational Research, Studies, and Analysis. Research, studies, and analysis done for educational purposes will post the same warning banner as the paper products, as follows. "The views expressed are those of the author and do not reflect the official policy or position of the U.S. Air Force, Department of Defense, or the U.S. Government."

14. Registration of Uniform Resource Locators. All web sites residing on Air Force systems, contracted using Air Force resources, or Air Force sponsored must register with Air ForceLINK at URL "http://www.af.mil/sites." The purpose of registering is to develop the Government Information Locator Service (GILS). At a minimum, register all web servers with Air ForceLINK and the MAJCOM web server administrator for inclusion in the master index of Air Force and MAJCOM web servers. Whenever there is a need to access a higher order list of servers, organizations will point to the applicable list rather than replicate the information.

15. Government Information Locator Service. The purpose of GILS is to provide a convenient, organized system for the public to access federal information resources. The Air Force point of entry into GILS is Air ForceLINK and its associated public access pages. All public access pages are required to develop an associated GILS Core Record. Office of Management and Budget (OMB) Bulletin 95-01, *Establishment of the Government Information Locator Service* describes GILS requirements; FIPS Publication 192, Application Profile for the Government Information Locator Service (GILS) describes mandatory and optional data elements required for the GILS Core Record. All Public Dissemination Products

(PDP), must have an associated GILS Core Record posted to Air ForceLINK. PDPs are information products produced by the Air Force specifically for the public. You do not need to convert PDPs to an electronic media and place them on Air ForceLINK; however, the GILS Core Record must reflect where to gain access to the PDP.

16. Records Management. Do not use internet pages or e-mail files to store official record copies of documents unless they contain an electronic records management application that manages the disposition of the records. Manage records according to AFMAN 37-123, *Management of Records*; AFI 37-138, *Records Disposition--Procedures and Responsibilities*; and AFMAN 37-139.

17. Electronic Mail. E-mail travels over the Non-secure Internet Protocol Router Network (NIPRNET) and other internet lines. Sending an e-mail is not considered placing or releasing information on the internet. E-mail is protected by passwords, direct addressing, and public law. Despite this protection, e-mail is vulnerable to interception. In addition, e-mail is recorded at the sending and receiving server. You must have access and security controls mentioned in **11**. in place to protect sensitive e-mail traffic. Determine the level of security measures required by the sensitivity of the information. Current e-mail packages do not guarantee delivery nor verify authenticity of the sender. To guarantee delivery, request a return receipt. To guarantee authenticity, verify information via telephone or additional e-mail. You can send non-critical unclassified sensitive information by using a password and user ID-protected e-mail. E-mail messages, including transmission data and attachments, may become official records, depending on the content of the message. Refer to records management publications listed in **16**. for guidance on managing e-mail as records.

JOHN S. FAIRFIELD, Lt General, USAF
DCS/Communications and Information

Attachment 1**GLOSSARY OF REFERENCES, ABBREVIATIONS, ACRONYMS, AND TERMS*****References***

AFI 10-1101, *Operations Security (OPSEC) Instructions*

AFI 31-401, *Managing the Information Security Program*

AFI 33-103, *Requirements Development and Processing*

AFI 33-113, *Telecommunications Centers and Data Processing Centers Management*

AFI 33-114, *Software Management*

AFI 33-115, *Networks Management*

AFI 33-127, *Electronic Messaging Registration and Authority*

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

AFI 35-205, *Air Force Security and Policy Review Program*

AFI 35-206, *Media Relations*

AFI 37-122, *Air Force Records Management Program* (will convert to AFI 33-322)

AFI 37-131, *Freedom of Information Act Program* (will convert to AFI 33-331)

AFI 37-132, *Air Force Privacy Act Program* (will convert to AFI 33-332)

AFI 37-138, *Records Disposition--Procedures and Responsibilities* (will convert to AFI 33-338)

AFI 61-204, *Disseminating Scientific and Technical Information*

AFMAN 37-123, *Management of Records* (will convert to AFMAN 33-323)

AFMAN 37-126, *Preparing Official Communications* (will convert to AFMAN 33-326)

AFMAN 37-139, *Records Disposition Schedule* (will convert to AFMAN 33-339)

AFPD 16-2, *Disclosure of Military Information to Foreign Governments and International Organizations*

AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*

AFPD 33-2, *C4 Systems Security*

AFPD 35-2, *Public Communications Programs*

AFPD 37-1, *Air Force Information Management* (will be converted to AFPD 33-3)

AFPD 61-2, *Management of Scientific and Technical Information*

AFSSI 5013, *Password Management* (to be converted to AFMAN 33-223)

AFSSM 5003, *Designated Approving Authority Guide*

AFSSM 5022, *Network Risk Analysis Guide*

Computer Fraud and Abuse Act of 1986.

DoDD 5200.28, *Security Requirements for Automated Information Systems (AIS)*

DoDD 5230.9, *Clearance of DoD Information for Public Release*

FIPS 140-1, *Security Requirements for Cryptographic Modules*

FIPS 192, *Application Profile for the Government Information Locator Service (GILS)*

OMB 95-01, *Establishment of the Government Information Locator Service*

Article 92, Uniform Code of Military Justice

Abbreviations and Acronyms

AFCA—Air Force Communications Agency

AFI—Air Force Instruction

AFIWC—Air Force Information Warfare Center

AFMAN—Air Force Manual

AFPD—Air Force Policy Directive

AFRES—Air Force Reserve

AFSSI—Air Force Systems Security Instruction

AFSSM—Air Force Systems Security Memorandum

AIS—Automated Information System

ANG—Air National Guard

BNCC—Base Network Control Center

CSO—C4 Systems Officer

CSSO—C4 Systems Security Officer

DAA—Designated Approving Authority

DoD—Department of Defense

DoDD—Department of Defense Directive

DRU—Direct Reporting Unit

DSN—Defense Switched Network

FIPS—Federal Information Processing Standards

FOA—Field Operating Agency

FOIA—Freedom of Information Act

FOUO—For Official Use Only

FTP—File Transfer Protocol

GILS—Government Information Locator Service

HTML—Hypertext Markup Language

HTTP—Hypertext Transfer Protocol
ID—Identification
IETF—Internet Engineering Task Force
IP—Internet Protocol
ISP—Internet Service Provider
LAN—Local Area Network
MAJCOM—Major Command
MAN—Metropolitan Area Network
MWR—Morale, Welfare, and Recreation
NIPRNET—Non-Secure Internet Protocol Router Network
NNTP—Network News Transfer Protocol
OMB—Office of Management and Budget
OPR—Office of Primary Responsibility
OPSEC—Operations Security
PA—Public Affairs
PDP—Public Dissemination Products
POC—Point of Contact
RDT&E—Research Development, Test, and Evaluation
rlogin—Remote Login
SAF—Secretary of the Air Force
SMTP—Simple Mail Transfer Protocol
SSL—Secure Sockets Layer
STINFO—Scientific and Technical Information
TCP/IP—Transmission Control Protocol/Internet Protocol
TDY—Temporary Duty
UCMJ—Uniform Code of Military Justice
URL—Uniform Resource Locator
USAF—United States Air Force
WWW—World Wide Web

Terms

Air ForceLINK—The official web information service for the Air Force.

Base Home Page—A public page that is the official base home page for an installation.

Client—A computer or program that requests a service of other computers or programs.

C4 Systems Officer (CSO)—The term CSO identifies the supporting C4 systems officer at all levels. At base-level, this is the commander of the communications unit responsible for carrying out base C4 systems responsibilities. At MAJCOM and other activities responsible for large quantities of C4 systems, it is the person designated by the commander as responsible for overall management of C4 systems budgeted and funded by the MAJCOM or activity. The CSO function uses the office symbol "SC" which is expanded to three and four digits to identify specific functional areas. CSOs are the accountable officers for all automated data processing equipment in their inventory.

DefenseLINK—An official web information service for the Department of Defense.

Designated Approving Authority (DAA)—Official with the authority to formally assume responsibility for operating an automated information system (AIS) or network at an acceptable level of risk.

File Transfer Protocol (FTP)—A protocol for file transfer between computers; transferring files efficiently and reliably among computers and allowing the convenient use of remote file storage capabilities. A transfer protocol used to transfer files from one computer to another.

Firewall—A protection scheme that assists in securing internal systems from external systems.

Gopher—An information transfer protocol based on a menu interface. Gopher is a distributed document search and retrieval system; it combines the best features of browsing through collections of information and fully indexed databases. The protocol and software follow a client-server model, and permits users on a heterogeneous mix of desktop systems to browse, search, and retrieve documents residing on multiple distributed server machines.

Home Page—A starting point or center of an infostructure on the WWW. A typical home page will consist of hypertext links (pointers) to other web documents.

Hypermedia—The extension of hypertext to things other than documents (for example, video and audio clips).

Hyperlink—A way to link access to information of various sources together within a web document. A way to connect two internet resources via a simple word or phrase on which a user can click to start the connection.

Hypertext—A method for storing, retrieving, and presenting information based on the processing power of computers. Allows computerized linking and almost instantaneous retrieval of information based on a dynamic index.

Hypertext Markup Language (HTML)—The native language of the WWW. HTML is a subset of the more complex Standard Generalized Markup Language (SGML).

Hypertext Transfer Protocol (HTTP)—It is the primary protocol used to communicate on the WWW.

Infostructure—A group of web documents linked together on one or more servers, usually providing information concerning a certain subject or idea.

Information Protection Office—Formerly C4 Systems Security Office (CSSO).

Information Provider—The person or organization that provides information for posting on the internet.

Internet—An informal collection of government, military, commercial, and educational computer networks using the Transmission Control Protocol/Internet Protocol (TCP/IP) to transmit information.

The global collection of interconnected local, mid-level, and wide area networks that use IP as the network layer protocol.

Internet Service Provider—A commercial entity providing data connectivity into the internet.

Intranet—A restricted-access network that works like the Web, but isn't on it. Usually owned and managed by an organization, an intranet enables a activity to share its resources with its employees without sensitive information being made available to everyone with internet access. Intranets may allow connection outside of the intranet to the internet through firewall servers and other security devices that have the ability to screen messages in both directions so that the organizations security is maintained.

Internet Protocol (IP) Spoofing—The use of software to change the address of a data packet to make it appear to come from another machine. Many network routers use these IP addresses to identify which machines have valid access rights to the network. Spoofing allows a hacker to "change his identity" and appear as a valid machine within the network. This type of attack can be foiled by the filtering router which drops "outside" packets with an "inside" source address.

Limited Access—Limited access of internet information applies to information that has been approved for limited access. This information has added safeguards that limit the access to a specific group or groups. According to AFI 35-205, the Office of Public Affairs (PA) will provide security and policy review for internet information at the OPR's request. The OPR must determine the appropriate security and access controls required to safeguard the information.

Limited Access by Domain—Limiting access by using the domain name (for example, .mil, .gov, .edu, and so forth) to restrict access of an area to a specific group or subgroup. Domains are established by the Internet Engineering Task Force (IETF) and assigned based on function or geography.

Limited Pages— Web pages intended for viewing by a limited audience.

Military Controlled Access Paths—Nonclassified networks or "links" that are leased, configured, managed, and secured by a government agency. This includes the unclassified but sensitive Internet Protocol Router Network (NIPRNET-AF, previously AFIN [Air Force Internet]) as well as dedicated links that have a node on the base network.

Network News Transfer Protocol (NNTP)—Also known as Usenet, specifies a protocol for the distribution, inquiry, retrieval, and posting of news articles using a reliable stream-based transmission of news among the internet community. NNTP is designed so that news articles are stored in a central database, allowing a subscriber to select only those items he wishes to read. Indexing, cross-referencing, and expiration of aged messages are also provided.

Page Maintainer—The creator and, or focal point for specific material posted on the organization's home page.

Proxy Server—A server connected to the internet through which all incoming and outgoing requests go through; used to enhance security and increase performance/efficiency.

Public Access—Public access of internet information applies to information approved for unlimited public release. Public access information has no access or security controls to limit access to the information. This review determines degree of releasability only; actual release of the material is the decision of the originator (OPR).

Public Dissemination Products (PDP)—Information products produced by the Air Force specifically for the public.

Public Pages—Web pages intended for viewing by the general public. Information on these pages should be of interest to the general public.

Scientific and Technical Information (STINFO)—STINFO includes all technical publications and documents generated by all Air Force-funded research development, test, and evaluation (RDT&E) programs, including working papers, memoranda, and preliminary reports, that DoD could decide to disseminate to the public domain. It also encompasses engineering drawings, standards, specifications, technical manuals, blueprints, plans, instructions, computer software and documentation, photograph, technical orders, databases, and any other information that which is usable or adaptable design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce any military or space equipment or technology concerning that equipment. It applies to recordings. It does not apply to cryptographic and communications security documents, communications and electronic intelligence, and other categories that the Director, National Security Agency, or the Chief, Central Intelligence Agency designates.

Secure Sockets Layer (SSL)—A security protocol that provides privacy over the internet. The protocol allows client/server applications to communicate, while preventing eavesdropping. Servers are always authenticated and clients are optionally authenticated.

Server—Software residing on an appropriate hardware platform (computer) that provides a service to other computers or programs, by satisfying client requests.

Simple Mail Transfer Protocol (SMTP)—The protocol used to send electronic mail on the internet.

TELNET—Also known as rlogin, TELNET starts a remote session by specifying a computer to connect to. The command and program used to log in from one internet site to another. The TELNET command/program gets you to the "login:" prompt of another computer or computer system. From that time until you finish the session, anything you type is sent to the other computer.

Transmission Control Protocol/Internet Protocol (TCP/IP)—The most accurate name for the set of protocols known as the "Internet Protocol Suite." TCP and IP are two of the protocols in this suite. Because TCP and IP are the best known of the protocols, it has become common to use the term TCP/IP or IP/TCP to refer to the whole family. TCP (the "transmission control protocol") is responsible for breaking up the message into datagrams, reassembling them at the other end, resending anything that gets lost, and putting things back in the right order. IP (the "Internet Protocol") is responsible for routing individual datagrams.

Trojan Horse—A malicious program designed to break security or damage a system that is disguised as something else benign, such as a directory list, archive, a game, or a program to find and destroy viruses.

Uniform Resource Locators (URL)—An internet "address" of a resource. URLs can refer to web servers, FTP sites, Gopher resources, News Groups, etc.

Web Browser—Software that acts as a client, allowing a person to retrieve information from various sources on the WWW.

Web Document—A physical or logical piece of information on the WWW.

Web Page— A single document that includes the text of the document, its structure, any links to other documents, images, and other media.

Web Server—A software/hardware combination that provides information resources to the WWW.

Web Server Administrator—The system administration for the web server, usually referred to as the

"Webmaster."

World Wide Web (WWW)—Uses the internet as its transport media and is a collection of protocols and standards that allow the user to find information available on the internet by using hypertext and/or hypermedia documents.

ATTACHMENT 2 (ADDED-AMC)**CHECKLIST FOR ESTABLISHING A WEB HOME PAGE**

A2.1. (Added-AMC) Setup user systems for access to the web (POC-WGM (Work Group Manager)).

A2.1.1. (Added-AMC) Trumpet Winsock (include FTP and Telnet Options) For Windows 95 machines, the Winsock is built into the operating system. Windows 95 users will need a separate FTP program such as WS-FTP LE.

A2.1.2. (Added-AMC) IP Address

A2.1.3. (Added-AMC) Web Browser

A2.2. (Added-AMC) Ensure Letter of Appointment for the Directorate Web Supervisor is on file with the Web Management Office (POC-Director of Directorate).

A2.3. (Added-AMC) Generate ticket request with the Base Help Desk to establish a Home Page. User account and space will be granted on the server (POC-AFNCC Help Desk/Web Management Office).

A2.4. (Added-AMC) Request HTML editor if needed (POC-AFNCC Help Desk/Web Management Office).

NOTE:

Customers may wish to submit an AF 3215 to purchase an HTML Editor such as Front Page, Hot Dog, etc., although note pad and Word 6.0 and up have HTML editors in them. HTML Editor availability through the AFNCC is extremely limited.

A2.5. (Added-AMC) Identify information type (Public access, FOUO, etc.).

NOTE:

You may need to obtain FOUO or FOIA release approval. Ensure release is documented and on file (POC-Wing or HQ AMC/SC FOIA Office).

A2.6. (Added-AMC) Sign the Risk Acceptance form and list restrictions you want on your Home Page. (Open, limited, password restricted, etc.). The commander or (2-digit)/designated representative must also sign this form (POC-Page Maintainer).

A2.7. (Added-AMC) Design the Home Page and obtain approval within your chain. Use the Home Page approval format (Atch 2) for this requirement (POC-Page Maintainer).

A2.8. (Added-AMC) Coordinate your site through PA if the information will be publicly releasable and accessible. (POC-Page maintainer/Wing or AMC Public Affairs Office)

A2.9. (Added-AMC) Maintain this checklist with a copy of the Risk Assessment and Home Page Approval forms.

A2.10. (Added-AMC) Base Visual Information (VI) Center should be your resource for any graphics to be placed on your pages. Using a graphic you downloaded from another web site may or may not be legal or meet the “professionally presented” requirements (AFI 33-129, paragraph 12). Part of VI’s mission is to do professional presentations. VI should review all base/unit home pages for legality, composition and graphic format prior to being posted on the web.

ATTACHMENT 3. (ADDED-AMC)

HOME PAGE APPROVAL PROCESS

A3.1. (Added-AMC) Prior to release, OPRs and Page Maintainers will coordinate and document the process used to review information destined for Internet release. Review processes may vary depending on the type and value of information being considered for release. At a minimum, the commander (wing units) or two-digit, designated representative (DR) (AMC Directorates), must view and approve all new information being placed on the Internet. Blanket reviews are generally not allowed, except for standard publications. Releasability of standard publications is normally determined prior to publication, so a blanket review and clearance for unclassified standard publications are sufficient. Information will also be reviewed, at a minimum, monthly to ensure information posted on the Internet is still valid. Whenever new information is posted to the Internet, a new Internet Release Package will be accomplished.

A3.2. (Added-AMC) Completed Internet Release Packages (this form, Risk Summary sheet and Web Home Page Checklist) will be maintained in the OPR's and/or Page Maintainer's official files until the corresponding information is removed from the Internet. Maintain these files according to AFMAN 37-139, Records Disposition Schedule. The OPR and/or Page Maintainer are accountable in the event of unauthorized disclosure of limited access information.

URL _____

Information Type (public, limited access): _____

Approval Date: _____ Page Maintainer Initials: _____ CC/2 Digit Initials/DR: _____

Review Date: _____ Page Maintainer Initials: _____ CC/2 Digit Initials/DR: _____

Review Date: _____ Page Maintainer Initials: _____ CC/2 Digit Initials/DR: _____

Review Date: _____ Page Maintainer Initials: _____ CC/2 Digit Initials/DR: _____

Review Date: _____ Page Maintainer Initials: _____ CC/2 Digit Initials/DR: _____

Page Maintainer: _____

Signature: _____

Directorate Web Supervisor: _____

Signature: _____

Commander/2 Digit/DR: _____

Signature: _____

Organization/Directorate: _____

**DR = Designated Representative

*Review at least every 30 days for accuracy

ATTACHMENT 4. (ADDED-AMC)**AMC WORLD WIDE WEB RISK SUMMARY**

A4.1. (Added-AMC) Purpose : The purpose of this summary is to identify the vulnerabilities, their impact, safeguards and residual risk (vulnerabilities remaining after implementation of security safeguards) to sensitive data stored on the WWW.

A4.2. (Added-AMC) System Summary : The WWW is designed to maximize the dissemination of command related information throughout the Air Mobility Command. This goal is accomplished by establishing a system where personnel at various locations around the world can access AMC related information through the Internet. The information accessible from the WWW will consist of public releasable and limited access (sensitive) data. Information in both of these categories will reside on the same hardware/software platform.

A4.3. (Added-AMC) Vulnerabilities : Access to the Internet increases the likelihood that a system will experience attempts to exploit its vulnerabilities. Typically, web servers experience a greater number of exploitation attempts because of the large community of interest they support. Common WWW vulnerabilities that can significantly degrade system operations and are often exploited include:

A4.3.1. (Added-AMC) Exploiting functional system services to obtain access to command privileges.

A4.3.2. (Added-AMC) Using malicious software (sniffer) to capture and/or crack user passwords to gain unauthorized access to limited access data.

A4.3.3. (Added-AMC) Gaining unauthorized system access by pretending to originate from a military or government address.

A4.3.4. (Added-AMC) Acquiring unauthorized privileges to modify system data.

A4.3.5. (Added-AMC) Covertly installing malicious software programs that degrade system performance or collect system data in order to obtain command privileges.

A4.4. (Added-AMC) Impact . Successful exploitation of the above vulnerabilities could impact the system and/or data as follows:

A4.4.1. (Added-AMC) Confidentiality. Limited access (sensitive) data could be divulged to unauthorized individuals who do not have a need-to-know. The unauthorized release of limited access data could adversely affect U.S. national interest, the conduct of DoD programs or the privacy of DoD personnel.

A4.4.2. (Added-AMC) Integrity. Public and limited access data may be modified or destroyed through unintentional or malicious acts.

A4.4.3. (Added-AMC) Availability. Authorized users could be denied access to the system and/or its data.

A4.5. (Added-AMC) Security Safeguards : Factors that must be taken into consideration when selecting security safeguards are to minimize the impact on system performance and impede the efforts of a determined hacker. Experience has proven that these goals cannot be accomplished through the imple-

mentation of a single solution. Security safeguards projected to mitigate the risks associated with the WWW operations will include a combination of procedural and system (automated) protection mechanisms. System protection mechanisms will focus primarily on restricting access to system privileges and limited access data to only those individuals with an official need-to-know who have been granted formal system access. System protection mechanisms will include password management, firewall protection, transmission protocol controls and audit and automatic lockout features. Procedural safeguards will comprise publishing security policy and documentation that defines the system security configuration and describes proper use of available security features.

A4.6. (Added-AMC) Residual Risk : Security safeguards cannot be implemented to totally eliminate the risk to the WWW without significantly impacting system performance. While the projected procedural and system safeguards are expected to minimize successful exploitation of the vulnerabilities cited above, system data owners should be aware that unauthorized disclosure of limited access data couldn't be ruled out. However, strict user compliance with published security policy will further reduce the possibility of unauthorized access to limited access data.

STATEMENT OF RISK ACCEPTANCE

I am the information owner for _____ . I require that restrictions be in place to limit my information to the following users:

I understand the threats to information placed on the (limited access) XXXXXX AFB World Wide Web and accept those risks.

Date: _____

Date: _____

Date: _____