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

*AIR FORCE INSTRUCTION 33-129*

*12 AUGUST 2004*

*Communications and Information*

# *WEB MANAGEMENT AND INTERNET USE*

**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 AFCA/ITXD (SMSgt Sandra Lyons)
Supersedes AFI 33-129, 4 April 2001

Certified by: HQ USAF/ILC (Mr. Richard L. Testa)
Pages: 45
Distribution: F

This Air Force instruction (AFI) implements Air Force Policy Directive (AFPD) 33-1, *Command, Control, Communications, and Computer (C4) Systems*; AFPD 33-2, *Information Protection* (will become Information Assurance); AFI 35-101*, Public Affairs Policies and Procedures*; and AFPD 37-1, *Air Force Information Management* (will become AFPD 33-3). This instruction provides policy and procedural guidance with respect to establishing, operating, and maintaining Web sites in the Air Force. It covers using 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. It defines the roles and responsibilities of all personnel who access, employ, and administer Web services. It outlines responsibilities and procedures for accessing information and properly establishing, reviewing, posting, and maintaining government information, pages, and sites on the Web. This instruction applies to all Air Force military, civilian, and contractor personnel, including Air National Guard (ANG) and Air Force Reserve Command (AFRC), and other users of the Air Force enterprise network. **Failure to observe the prohibitions and mandatory provisions of this instruction as stated in paragraph 2.2. by military personnel is a violation of the *Uniform Code of Military Justice (UCMJ),* Article 92, Failure to Obey Order or Regulation. Violations by ANG military personnel may subject members to prosecution under their respective State Military Code or result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws. Violations by civilian employees may result in administrative disciplinary action without regard to otherwise applicable criminal or civil sanctions for violations of related laws**. Violations by contactor personnel will be handled according to local laws and the terms of the contract. Ensure that all records created as a result of processes prescribed in this instruction are maintained in accordance with Air Force Manual (AFMAN) 37-123, *Management of Records*, and disposed of in accordance with the Air Force Web-RIMS Records Disposition Schedule (RDS) located at **https://webrims.amc.af.mil/rds/index.cfm**. Public Law 104-13, *Paperwork Reduction Act of* 1995, and AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*, affect this publication. Refer recommended changes and conflicts between this and other publications to

Headquarters Air Force Communication Agency (HQ AFCA/ITXD), 203 W. Losey St., Room 1100, Scott AFB IL 62225-5222, through appropriate channels, using AF Form 847, **Recommendation for Change of Publications**. See Attachment 1 for a glossary of references and supporting information.

## *SUMMARY OF REVISIONS*

**This document is substantially revised and must be completely reviewed.**

The changes include changing the publication's title to *Web Management and Internet Use*, which reflects the Air Force's policy on appropriate Internet use; the addition of compliance with the Rehabilitation Act of 1973; restrictions on the use of "cookies"; and updates or establishes roles and responsibilities for all persons or offices involved in the Web development or administration process. It requires Web Server Administrators, Web Masters, and Network Control Centers/Network Operations and Security Centers (NCC/NOSC) to continually ensure the Web is effectively and securely employed; and requires the training of all Web Server Administrators and Web Page Maintainers prior to performing respective Web management roles. This revision provides clarification for republishing base newspapers on the Web and refines policy pertaining to removal of personally identifying information, privacy and security notices, and warning and restriction banner wording. It updates review procedures for posting information on the Web, establishes guidance on official Air Force Web sites outside the military (.mil) domain, and initiates routine security measures for Web servers. Incorporates Deputy Secretary of Defense-issued communications bandwidth policies. Deletes the requirement to include a Comment Form with Privacy and Security Notice banner. It incorporates the Director, Administration and Management Memorandum, *Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA)*, November 9, 2001, and AF-CIO Policy Memorandum 03-01, *Web Site Policy*, January 28, 2003, into this instruction.

**1. Purpose.** Use of the World Wide Web (WWW) or Web technologies continues to increase as a technique for obtaining and disseminating information worldwide. The Web/Internet provide the capability to quickly and efficiently disseminate information to and access information from a variety of governmental and nongovernmental sources. The Air Force maintains/supports two types of Web pages/sites. The first is Air Force Public Web Pages/Sites that are intended for viewing by the general public via the Internet, and the information on these pages must be of interest to the general public. The second is Air Force Private Web Pages/Sites, they are intended for a limited audience, specifically .mil and .gov users. Information on private Web pages/sites must consider the access and security controls.

**2. Use of Internet Resources by Government Employees.** The Internet provides an indispensable source for information from a variety of governmental and nongovernmental sources. The Air Force goal, within acceptable risk levels, is to provide personnel requiring access for official business maximum accessibility to Internet resources.

2.1. Appropriate Use. Government-provided hardware and software are for official use and authorized purposes only. Appropriate officials may authorize personal uses consistent with the requirements of DOD 5500.7-R, *Joint Ethics Regulation (JER*), after consulting with their ethics counselor. Such policies should be explicit, as unofficial uses that exceed the authorized purposes may result in adverse administrative or disciplinary action.

2.2. Inappropriate Use. Using the Internet for other than official or authorized purposes may result in adverse administrative or disciplinary action. The activities listed in paragraphs **2.2.1.** through **2.2.14.** involving the use of government-provided computer hardware or software are specifically prohibited.

2.2.1. Use of Federal government communications systems for unauthorized personal use.

2.2.2. Uses that would adversely reflect on the Department of Defense (DOD) or the Air Force such as chain letters, unofficial soliciting, or selling except on authorized bulletin boards established for such use.

2.2.3. Unauthorized 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; sexually harassing materials, pornography and other sexually explicit materials.

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

2.2.5. Using copyrighted material in violation of the rights of the owner of the copyrights. Consult with the servicing Staff Judge Advocate for “fair use” advice.

2.2.6. Participating in non-DOD or nongovernment “chat lines,” “chat groups,” or open forum discussion to or through a public site, unless it is for official purposes and approved through the Global Information Grid (GIG) Waiver Board.

2.2.7. Unauthorized use of the account or identity of another person or organization.

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

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

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

2.2.11. Permitting an unauthorized individual access to a government-owned or government-operated system.

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

2.2.13. Copying and posting official information to unauthorized Web sites.

2.2.14. Downloading and installing freeware/shareware or any other software product without Designated Approving Authority (DAA) approval.

## 3. Roles and Responsibilities.

3.1. Assistant Secretary of the Air Force for Acquisition (SAF/AQ). Deputy Assistant Secretary of the Air Force (Contracting) (SAF/AQC) develops, in coordination with Secretary of the Air Force Office of Public Affairs (SAF/PA), policy and guidance governing the review and release of contracting-related information made available on public Web sites in the conduct of electronic commerce (e.g., Requests for Proposals, Federal Business Opportunities notices, etc.).

3.2. Air Force Chief Information Office (AF-CIO). The AF-CIO will:

3.2.1. Develop information management policy and guidance governing the Web.

3.2.2. Develop and promulgate policy relating to the management and use of Web resources.

3.2.3. Develop and ensure the establishment of a common infrastructure upon which all Air Force Web sites, pages, content, etc., will be installed and maintained.

3.2.4. Develop and promulgate policy to ensure that developed Web resources maximize the use of common enterprise tools and promote sharing of data, knowledge, and information throughout the Air Force corporate structure.

3.2.5. Ensure that an annual multidisciplinary review is conducted of all public Web sites to comply with current guidance.

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

3.3.1. Develop policy and guidance governing the public communication program and the security and policy review program.

3.3.2. Develop policy and guidance for the integration of public Web sites into Air Force public communication plans and programs.

3.3.3. Develop a public Web site review process for posting information on public Web sites.

3.3.4. Ensure all Air Force public Web sites are registered on Air Force Link.

3.3.5. Serve as public Web site point of contact (POC) for routine reports submitted by Web Risk Assessment Cells, which are responsible for vulnerability analysis and threat assessments of Air Force Web site content.

3.3.6. Chair the Annual Multidisciplinary Review Board. Initiate annual multidisciplinary reviews of all public Web sites, and send results to AF-CIO. Complete these reviews during Information Assurance Awareness Month. Site reviews identify information considered sensitive from the operational, public affairs, acquisition, technology, privacy, legal, and security perspectives; ensure compliance with DOD Web Privacy policies; and assure Air Force Link and Government Information Locator Service (GILS) registrations are consistent. Coordinate these reviews across organizational boundaries as necessary (both vertically and horizontally), to ensure critical information is consistently controlled and up-to-date. Where ANG units are involved, coordination must include the respective State Adjutant General.

3.4. Headquarters United States Air Force, Deputy Chief of Staff for Air & Space Operations (HQ USAF/XO). The Director of Intelligence, Surveillance, and Reconnaissance, Deputy for Information Warfare (HQ USAF/XOIW) will:

3.4.1. Develop policy and guidance on the review of operationally sensitive information on Air Force Web sites.

3.4.2. Serve as POC for routine reports submitted by Web Risk Assessment Cells, which are responsible for vulnerability analysis and threat assessments of Air Force public and private Web site content.

3.5. Headquarters United States Air Force, Deputy Chief of Staff for Installations and Logistics (HQ USAF/IL). The Directorate of Communications Operations (HQ USAF/ILC) will:

3.5.1. Develop implementation guidance on the operation, maintenance, and security of the systems that facilitate the use of the Web, including guidance on persons with disabilities with regard to use and access to the Web.

3.5.2. Initiate an annual review for the configuration/architecture of hardware and software used in the operation and security of Air Force Web sites.

3.5.3. Develop and maintain training standards for personnel involved in Web page development.

3.5.4. Participate in the annual multidisciplinary reviews of all Air Force public Web sites (see paragraph **3.3.6.**).

3.5.5. Initiate the first review and approve all Air Force Non-Secure Internet Protocol Router Network (NIPRNET) waiver requests for submittal to the Defense Information Systems Network (DISN) Security Accreditation Working Group (DSAWG) and the GIG Waiver Board.

3.6. Headquarters Air Education and Training Command (HQ AETC) and the United States Air Force Academy (USAFA). As Air Force educational institutions, HQ AETC and USAFA will comply with Department of Defense Directive (DODD) 5230.9, *Clearance of DOD Information for Public Release*, April 9, 1996; and AFI 35-101. While ensuring students and faculty are provided the necessary latitude to conduct research or scientific collaborations, it is prohibited to connect .edu domain Web servers or related educational network traffic to the .mil (NIPRNET) architecture (i.e., dual home to the .edu domain to the .mil domain) unless physical or logical mitigations are approved and put in place.

3.7. Major Commands (MAJCOM)/Field Operating Agencies (FOA)/Direct Reporting Units (DRU). MAJCOMs/FOAs/DRUs will ensure their respective headquarters organization and subordinate units comply with this instruction. They will:

3.7.1. Establish policy and procedures for content and appearance of public Web sites according to AFI 35-101.

3.7.2. Establish procedures for creation, maintenance, and review of command-wide private Web sites.

3.7.3. Ensure Operations Security (OPSEC) programs are effectively adhered to in accordance with AFI 10-1101, *Operations Security*.

3.7.4. Establish and maintain public Web sites outside the firewall and private Web sites inside the firewall. A waiver may be submitted for special consideration of unique circumstances impacting an organization's ability to meet this requirement. Please contact HQ USAF/ILCO, 1030 Air Force Pentagon, Washington DC 20330-1030, DSN 425-7820, for further details.

3.7.4.1. To maintain the security, integrity, and accountability of Air Force information on the Web, host all public and private Air Force Web sites in the .mil domain. Any Air Force Web site hosted on a commercial server (outside the .mil community) requires HQ USAF/ILC, AF-CIO, and DOD Chief Information Officer approval. Final approval resides with the DOD GIG Waiver Board. HQ USAF/ILCO will present the request to the DOD GIG Waiver Board. This also applies to nonappropriated (NAF)-commercial Web sites.

3.7.4.2. Air Force Reserve Officer Training Corp detachments and Air National Guard units may post their Web sites on their host institution/state-operated Web servers. Web sites must comply with the content related provisions of this instruction.

3.7.5. Control content on public sites through the Public Affairs (PA) office.

3.7.6. Ensure the PA offices register their respective public Web sites on Air Force Link.

3.7.7. Provide an index of their subordinate organizations' public home pages through Air Force Link.

3.7.8. Ensure wing/base PA offices review all public Web sites prior to their launch. ANG units will coordinate with their unit Public Affairs Officer (PAO) prior to their launch. ANG geographically separated units use their host wing for PAO support.

3.7.9. Collect and review Annual Multidisciplinary Review Board results for all public Web sites and forward to SAF/PA or their designated representative. [Report control symbol (RCS) SAF-PAS(A) 0203]

3.7.9.1. Establish a follow-up system to ensure corrective actions are implemented.

3.7.10. Accept responsibility for and perform applicable duties from paragraphs **3.8.** and **3.9.** when wing-level commanders or PA offices do not fulfill those duties.

3.8. Wing commanders or equivalents will:

3.8.1. Maintain responsibility for the content and security of the information posted on their public and private Web pages/sites.

3.8.2. Publish local policy and guidance defining authorized personal use of the Internet.

3.8.3. Ensure review and approval of information (in accordance with SAF/PAAQ guidance) made available on their respective public Web sites for the conduct of electronic commerce. Ensure local clearance and approval procedures for posting information to the Internet/public Web sites comply with AFI 35-101.

3.8.4. Ensure Wing PA office reviews all their respective public Web pages/sites prior to their launch.

3.8.5. Ensure a process (consistent with this instruction) is in place to establish and maintain Internet Release Packages (IRP) for their organization's private Web sites.

3.8.6. Ensure that installation PA offices annually conduct multidisciplinary reviews of all public Web sites.

3.8.7. Ensure For Official Use Only (FOUO) information is properly protected and not posted on public Web sites.

3.8.8. Ensure public Web sites comply with privacy policies regarding restrictions on persistent and third party cookies, and add appropriate privacy and security notices at major Web site entry points and Privacy Act statements or Privacy Advisories when collecting information. (See paragraph **9.** for additional guidance on cookies.)

3.8.9. Ensure installation public Web sites have the required Freedom of Information Act (FOIA) page according to DOD 5400.7-R/Air Force Supplement 1 (AFSUP1), *DOD Freedom of Information Act Program*.

3.8.10. Ensure the Communications and Information Systems Officer (CSO) inactivates Web sites with inappropriate or sensitive postings until the issue is resolved.

3.8.10.1. Inappropriate Information—the inclusion of FOUO information on an official Web site that is accessible to the general public. Examples include, but are not limited to, unit recall rosters, detailed budget reports, scheduled military operations, etc.

3.8.10.2. Sensitive Information—the disclosure of information that would cause foreseeable harm to an interest protected by one or more of the exemptions to the FOIA, or the release of which would be a clearly unwarranted invasion of personal privacy. Examples include unclassified information about classified programs, dates of birth, Social Security Numbers (SSN), etc.

3.8.11. Ensure corrective actions are implemented for posting inappropriate information to public Web sites, failure to comply with privacy policy, and other Web site and server violations.

3.8.12. Ensure the Notice and Consent banner is placed on each Web page. Providing a statement such as "Please read this privacy and security notice" linked to the actual notice is satisfactory.

3.9. Wing-level or equivalent PA offices will:

3.9.1. Establish and chair Annual Multidisciplinary Review Boards which will consist of representatives from communications and information, Privacy Act, legal, contracting, operations security (OPSEC), and other representatives necessary to address questions concerning the sensitivity of information on installation public Web sites. The boards will:

3.9.1.1. Perform reviews that check public Web sites to ensure sensitive information from the operational, public affairs, acquisition, technology, privacy, legal, or security perspective is not present.

3.9.1.2. Ensure public Web sites comply with privacy policies regarding restrictions on persistent and third party cookies, and add appropriate privacy and security notices at major Web site entry points and Privacy Act statements or Privacy Advisories when collecting personal information.

3.9.1.3. Ensure that all public Web sites/pages comply with current laws and policies. (See paragraph **9.** for additional guidance on cookies).

3.9.1.4. Use AF IMT 2519, **All Purpose Checklist**, and criteria listed at **Attachment 3** to complete public Web site evaluations. You may download AF IMT 2519 from the Air Force Publishing Web site at **http://www.e-publishing.af.mil**.

3.9.1.5. Register public Web sites with Air Force Link.

3.10. Unit Commanders. Commanders are responsible for the content of the information posted on their public and private Web pages/sites. They will:

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

3.10.2. Submit Web services requirements (via AF IMT 3215, **IT/NSS Requirements Document**) to the CSO for approval and processing according to AFI 33-103, *Requirements Development and Processing*.

3.10.3. Obtain all Internet connectivity through the supporting base/installation CSO.

3.10.4. Ensure their Web Server Administrators, Web Masters, Web Page Maintainers and Information Providers receive training on topics that include, but are not limited to, OPSEC, Privacy Act, FOUO, and computer-based training on Web Administration at **https://usaf.smartforce.com/**.

3.10.5. Initiate and sign/approve appointment letters for their Web Server Administrators, Web Masters, and Web Page Maintainers (see **Attachment 4**).

3.10.5.1. Web Server Administrators will maintain appointment letters for their respective Web Masters and Web Page Maintainers.

3.10.5.2. Web Server Administrators' appointment letters will be maintained by the CSO.

3.11. Base/Installation CSO. The CSO will:

3.11.1. Efficiently manage base/installation Internet facilities to ensure procuring, using, and maintaining only authorized equipment and software necessary to perform official government business.

3.11.2. Ensure that all Web servers have a current and approved Certification and Accreditation before they are connected to the network (AFI 33-202, *Network and Computer Security*).

3.11.3. Coordinate with the Base Network Control Center (NCC) or MAJCOM Network Operations Security Center (NOSC) to perform security scans for all Web servers. Security scan will include the operating system and the Web applications running or installed on the Web servers. Report vulnerabilities to the associated Web Server Administrator for resolution.

3.11.4. Coordinate with the Base NCC or MAJCOM NOSC to deny access to any Web site/page/server that is or has the potential of being an operational or computer security risk or contains inappropriate or sensitive material. Web site/page access will be reinstated when issue is resolved.

3.12. Web Server Administrator is the POC for all matters relating to a Web server's physical access/login/accounts, maintenance, administration and is responsible for:

3.12.1. Maintaining security and access control features.

3.12.2. Maintaining configuration management of the Web server.

3.12.3. Granting and monitoring Web Master and Web Page Maintainer access privileges.

3.12.4. Configuring, maintaining, and evaluating audit control logs (AFI 33- 202*)*.

3.12.5. Gathering and analyzing performance data on servers under their control. Use this data to monitor utilization, response times, and server efficiency.

3.12.6. Ensuring certification and accreditation of their Web server before connecting to the network, as well as developing, coordinating, publishing, maintaining, and testing support plans for contingency and service restoration.

3.12.7. Ensuring user identifications (userid) and passwords comply with AFMAN 33-223, *Identification and Authentication.*

3.12.8. Coordinating with Web Masters and Web Page Maintainers to ensure compliance with all laws and policies such as in Title 42, U.S.C., Section 508, *Rehabilitation Act of 1998*; and Office of Management and Budget (OMB) policy on the use of cookies (see paragraph **9.** for additional guidance on cookies).

3.12.9. Operating, maintaining, and administering the server, to include system back-ups and disaster recovery.

3.13. Web Master. This individual is charged with posting information to the Web server. Specifically, Web Master responsibilities include:

3.13.1. Establishing a process for Web Page Maintainers to submit Web pages and ensuring compliance with established style, content, and security guidelines.

3.13.2. Preventing user access to Web sites under construction. Invalid attempts to access restricted Web pages will not include language like “Access Denied” or “Forbidden.”

3.13.3. Web Masters may support activities such as the Top 3, Chiefs' Group, local Union, etc., if approved by the DAA, Staff Judge Advocate (if available), or the legal office provided the resources are available. Submit a written request for these nonmission related activities justifying their requirement to the base/installation communications unit and ensure compliance with all policies and regulations regarding Web use and content. Pages listing personal information (i.e., hobbies, family photos, resumes, etc.) beyond the official duties and position of the individual are inappropriate and prohibited. They must follow the same guidance, policies, and laws imposed on private and public pages.

3.14. Web Page Maintainer. Each unit supplying Web page information for posting on the Web server appoints and trains a Web Page Maintainer responsible for information on their respective pages. The Web Page Maintainer is also responsible for:

3.14.1. Overseeing unit Web page development and maintenance. Ensure compliance with all laws and policies such as in Title 42, U.S.C., Section 508, *Rehabilitation Act of 1998*; and OMB policy on the use of cookies (see paragraph **9.** for additional guidance on cookies).

3.14.2. Establishing security and access control requirements before posting information on the Web.

3.14.3. Validating all links on Web pages within their span of control.

3.14.4. Ensuring the Information Provider performed the proper reviews and documented the process in accordance with paragraph **8.**, and AFI 35-101.

3.14.5. Identifying and updating incorrect or superseded information.

3.14.6. Maintaining the original completed IRP (**Attachment 2**) until the corresponding information is removed from the Web server. The Information Provider is accountable in the event of unauthorized disclosure of information.

3.14.7. Working with the Web Master to remove or correct instances of sensitive or inappropriate information on Web pages.

3.14.8. Ensuring Public and Private Web pages comply with Title 42, U.S.C., Section 508, *Rehabilitation Act of 1998* (refer to **http://www.access-board.gov/sec508/guide/1194.22.htm**).

3.15. Information Providers, the persons or organizations who provide information for posting on public or private Web pages and are responsible for the content, coordination, and classification of that information, will:

3.15.1. Ensure proper review and approval of material by the appropriate offices (see paragraph **8.** and AFI 35-101) and document via IRP (see **Attachment 2** or **Attachment 3**).

3.15.1.1. Account for the classification, currency, sensitivity, and release of the information.

3.15.2. Validate the accuracy of all material provided to the Web Page Maintainer.

3.15.3. Comply with Privacy Act requirements (i.e., safeguard personal information, post Privacy Act statement and Privacy Advisories) when collecting information from individuals. See paragraph **9.** for specific guidance on persistent cookies. (See AFI 33-332, *Air Force Privacy Act Program*).

## 4. Access to the Internet.

4.1. Commercial Internet Service Providers (ISP). Do not connect or subscribe to commercial ISPs for official E-mail or network services. Commercial ISP service can only be obtained via waiver from HQ USAF/ILC and the DOD GIG Board. Waiver requests shall explain how the other than NIPRNET internet connections meet the minimum security standards established by the DSAWG and be accompanied by a plan to transition the connection to the NIPRNET.

4.2. Quality-of-Life (QoL) Internet Services. The NCC may establish access for "patron" QoL activities such as the Family Support Center, library, and other Services/Morale, Welfare and Recreation (MWR) Category A, B, and C activities (defined in AFI 65-106, *Appropriated Fund Support of Morale, Welfare, and Recreation (MWR) and Nonappropriated Fund Instrumentalities (NAFIS)*). These systems shall not be connected to the base network with the privileges of ".af.mil" registered users. However, official business activities in these QoL locations may require and are authorized NIPRNET connectivity through the base network.

4.3. DOD Dependent Schools and Base Education Offices. Only government personnel and/or government contractors are authorized Web access through NIPRNET. Web access for classroom education or civilian education institutions must be through a commercial ISP; the commercial ISP connection cannot be connected to a NIPRNET circuit without a waiver. Please see CJCSM 6510.01, *Defense-in Depth: Information Assurance (IA) and Computer Network Defense (CND)*, for guidance on mobile code use.

**5. Web Page/Site Architecture.**

5.1. Public Web Pages/Sites. Public pages/sites are intended for viewing by the general public, and the information on these pages must be of interest to the general public. Uniform resource locator (URL) addresses will follow the standard protocol used throughout the Web (e.g., a site representing all of Dover Air Force Base to the public would most logically be located at **http://www.dover.af.mil**). Each installation and MAJCOM will only have one official public Web site. Please refer to the guidance listed in **Table 1.** and **Table 2.** to apply the appropriate security measures to the Web sites.

5.1.1. Private Web Pages/Sites. Private Web pages/sites are intended for a limited audience, specifically .mil and .gov users. Information on private Web pages/sites must consider the access and security controls. Please refer to the guidance listed in **Table 1.** and **Table 2.** to apply the appropriate security measures to the Web sites.

5.1.2. All unclassified, private DOD Web sites will be enabled to use Class 3 and/or Class 4 certificates, as applicable, for server authentication and client/server authentication.

5.2. External Links.

5.2.1. Links to non-.gov/-.mil Web resources should support the organization's mission. Review external links quarterly to ensure their continued suitability.

5.2.2. Product endorsements or preferential treatment on official DOD Web sites is prohibited according to DOD 5500.7-R.

5.2.2.1. Payment or compensation of any kind in exchange for a link placed on an organization's official DOD public or private Web site is prohibited. This does not preclude links provided to commercial sponsors or paid advertisers on NAF-commercial Web sites.

5.2.2.2. Public DOD Web sites will not require or encourage users to choose any specific browser software (DOD 5500.7-R). Additionally, official DOD public Web sites will not use graphics or logos depicting companies or products and should only use text or hyperlinks to the software site when absolutely needed to support the organization or its mission.

5.2.2.3. When using "frames" technologies, Web site owners will ensure "frames" are discontinued when links external to the site are activated.

5.2.2.4. Organizations may link to nonmission-related government activities, such as the Army and Air Force Exchange Service, the Navy Exchange Service Command, and the Marine Corps Exchange, with the approval of the DAA and legal office.

5.2.3. Use the following disclaimer when displaying commercial advertisements, sponsorships, or linking to nongovernment sites:

"The appearance of hyperlinks does not constitute endorsement by the U.S. Air Force or the information, products, or services contained therein. For other than authorized activities such as military exchanges and morale, welfare and recreation sites, the U.S. Air Force does not exercise any editorial control over the information you may find at these locations. Such links provided are consistent with the stated purpose of this DOD Web site."

This disclaimer may appear on the page or pages listing external links or through an intermediate "exit notice" page generated by the server machine whenever a request is made for any site other than an official DOD Web site (usually the .mil domain). This does not preclude links provided to commercial sponsors or paid advertisers on NAF-commercial Web sites.

5.2.4. Web Pages Funded With Nonappropriated Funds (NAF). To communicate Services' MWR activities and the availability of goods and services they offer to authorized patrons, NAF commercial ".com" Web sites may be established according to paragraph **3.7.4.1.** If resources are available, official DOD public Web sites may host NAF Web pages. Official DOD Web sites may provide hyperlinks to these NAF commercial Web sites; however, the NAF commercial Web sites may not provide hyperlinks to official DOD Web sites. Since MWR programs may have commercial sponsors, sponsor recognition may be provided on NAF-funded commercial Web sites, and this recognition may include hyperlinks to sponsor commercial Web sites subject to inclusion of appropriate disclaimers.

**Table 1. Security for Information Placed on Web Sites.**

| Types of Pages | Governing Publications | Review Process Includes: | Minimum Access/ Security Controls |
|---|---|---|---|
| Public (see Note 2) | AFI 35-101<br>AFI 10-1101<br>AFI 33-332<br>AFI 33-202<br>DOD 5400.7-R/AF Sup | PA<br>OPSEC Office<br>FOIA/Privacy Act Office<br>Foreign Disclosure Office (see Note 1)<br>Contracting (see Note 3)<br>Legal (see Note 3)<br>Information Security Manager<br>Unit Commander or Equivalent | Unlimited/ Unencrypted |
| Private (see Notes 1, 2, 5 and 6) | AFI 10-1101<br>AFI 33-332<br>AFI 33-202<br>AFI 33-219<br>DOD 5400.7-R/AF Sup | OPSEC Office<br>Privacy Act Office<br>Foreign Disclosure Office (see Note 3)<br>Legal (see Note 3)<br>Contracting (see Note 3)<br>Information Security Manager<br>Unit Commander or Equivalent | Public Key Infrastructure (PKI) User Certificates and/or User ID/Password through Proxy Server |
| Classified (see note 4) | DOD 5200.1-R, *Information Security Program*, January 1997<br>AFI 31-401, *Information Security Program Management*<br>AFI 33-219 | Information Security Manager | SIPRNET and User ID/Password |

***NOTES:***

1. Certain types of information, though unclassified, may still have restrictions of foreign access. If this possibility exists, consult AFI 33-202 and your local Foreign Disclosure Office for assistance. When the possibility of information becoming sensitive when aggregated with other nonsensitive information exists, the office of primary responsibility (OPR) should consult DOD O-5200.1-I, *Index of Security Classification Guides*, September 1996, and/or OPSEC office for assistance.

2. Review Scientific and Technical Information (STINFO) in accordance with guidance contained in AFPD 61-2, *Management of Scientific and Technical Information*, and AFI 61-204, *Disseminating Scientific and Technical Information*. Distribution Statement A requires no security controls; Distribution Statements B through F require Public Key Infrastructure (PKI) Certificates and/or User ID/password and encryption controls.

3. Optional review depending on type of information.

4. The following types of classified information may not be displayed on the Secret Internet Protocol Router Network (SIPRNET): Top Secret, classified information carrying a Special Access Required caveat, classified information carrying a Sensitive Compartmented Information (SCI) caveat, classified information containing a North Atlantic Treaty Organization (NATO) classification, classified information containing a Critical Nuclear Weapons Design Information (CNWDI) caveat, and information containing a Department of Energy Sigma caveat.

5. When Private sites/pages are initially established, the full review process is required. Changes or updates to those pages/sites only require commander or equivalent review and approval.

6. Names and e-mail addresses may be posted to .mil restricted Web sites for official purposes if authorized by the local commander and after performing an appropriate risk assessment.

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

| Types of Pages | If Access Control is: | and Security Control is: | the Vulnerability is: | and the Web Documents will be those that are: |
|---|---|---|---|---|
| Public | Unlimited | Unencrypted | **EXTREMELY HIGH**--open to everyone on the Internet worldwide. | Publicly accessible, including some STINFO marked "Distribution Statement A." |
| Public | Internet Domain (e.g., *.mil*, *.gov*) or Internet Protocol (IP) Address | Unencrypted | **HIGH**--Can spoof access controls; affords the lowest level of access control; and no encryption. | Nonsensitive. Normally publicly accessible; OPR prefers material remain outside of public view. |
| Public | 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. | Nonsensitive. Private to small groups; OPR prefers protection of material with higher confidence of security. |
| Private | Internet Domain (e.g., *.mil, .gov*) or Internet Protocol (IP) Address | Encrypted | **LOW**--Provides encryption and the lowest level of access control. | Sensitive. Lists of names and e-mail addresses (directories, org charts, rosters, etc.). OPR prefers material protected with high confidence of security. |
| Private | 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. |

**6. Page Layout and Maintenance.** Organizations must ensure Web pages are professionally presented, current, accurate, factual, related to the organizational mission, and follow the guidance and policy as described in paragraph **5.1.** Use images appropriate to the content; do not use images indiscriminately. Do not display hyperlinks to incomplete paths or use the phrase "under construction"; additionally, do not introduce information or services until they are ready. Announce new or substantially changed information on the home page. Institute of Electrical and Electronics Engineers (IEEE) Standard 2001, *IEEE Recommended Practice for Internet - Web Site Engineering, Web Site Management, and Web Site Life Cycle*, 2002, define recommended practices for (WWW) page engineering for Intranet and Extranet environments, based on World Wide Web Consortium (W3C) and related industry guidelines. Web Page Maintainers will ensure the data in their area of responsibility is date/time stamped to reflect the most current information. At a minimum, base and organization (e.g., wing, group, squadron, special staff agencies, etc.) Web pages must comply with Hypertext Markup Language (HTML) 4.0 specifications and contain information described below:

6.1. Private Web Pages.

6.1.1. The following information is only required at the top-level page.

6.1.1.1. Web Page Maintainer's organization, office symbol, commercial phone number, and Defense Switched Network (DSN) phone number.

6.1.1.2. Organizational e-mail address.

6.1.1.3. Date last reviewed (pages/links must be reviewed at least every 180 days).

6.1.2. The following information is required on every page:

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

6.1.2.2. Warning banners (or links to) as indicated in paragraph **7.2.**

6.1.2.3. Link to organization home page.

6.1.2.4. Notice and Consent banner as required in AFI 33-219.

6.2. Public Web Pages:

6.2.1. The following information is only required on each unit or organizational top level page:

6.2.1.1. Organizational name and shield.

6.2.1.2. Organization, office symbol, and commercial phone number.

6.2.1.3. Organizational e-mail address.

6.2.1.4. Date Last Reviewed (pages/links must be reviewed at least every 180 days).

6.2.1.5. Link to Air Force Link.

6.2.1.6. Notice and Consent banner is placed on each Web page.

6.2.2. The following information is required on every page:

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

6.2.2.2. Link to organization home page.

6.2.2.3. Privacy and Security Notice and Warning banners (or links to) as indicated in paragraph **7.1.**

6.3. SIPRNET Web pages:

6.3.1. The following information is only required at the top-level page.

6.3.1.1. Web Page Maintainer’s contact link.

6.3.1.2. Organizational name. Shields may be included if bandwidth allows.

6.3.1.3. Web Page Maintainer's organization, office symbol, commercial phone number, and

DSN phone number.

6.3.1.4. Organizational e-mail address.

6.3.1.5. Date last reviewed (pages/links must be reviewed at least every 180 days).

6.3.1.6. Notice and Consent banner as required in AFI 33-219.

6.3.2. The following information is required on every page:

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

6.3.2.2. Warning banners (or links to) as indicated in paragraph **7.2.**

6.3.2.3. Link to organization home page.

6.3.2.4. Applicable security markings for each document, link, and item (including unclassified information).

6.3.3. There will be no links to pages/sites outside the SIPRNET.

6.4. Meta-Indexes, Indexes, or Lists of Other Air Force and DOD Pages. Indexes and lists will only reside on MAJCOM sites or on the Air Force Link, the Air Force's service-level site. Base level home pages will refer to these centralized lists. Send additions, deletions, and changes to the Air Force index via e-mail to the address listed on Air Force Link. MAJCOMs will extract their portion of the list from the Air Force Link index. Indexes and lists are limited to those sites that provide relevant information to the intended audience.

6.5. Personally Identifying Information.

6.5.1. Public Web Site Information. Do not place personally identifying information for DOD personnel on public Web sites. This applies to unclassified public Web sites regardless of domain (e.g., .com, .edu, .org, .mil, .gov) or sponsoring organization (e.g., Non-Appropriated Fund/Morale, Welfare and Recreation sites; DOD educational institutions). Personally identifying information includes name, rank, e-mail address, and other identifying information regarding DOD personnel, including civilians, active duty military, military family members, contractors, members of the National Guard and Reserves, and Coast Guard personnel when the Coast Guard is operating as a service in the Navy. Rosters, directories (including telephone directories) and detailed organizational charts showing lists of names (or e-mail addresses) are considered personally identifying information and are FOUO. Multiple names of individuals from different organizations/locations listed on the same document or Web page constitutes a list. Aggregation of names across pages must specifically be considered. In particular, the fact that data can be compiled easily using simple Web searches means caution must be applied to decisions to post individual names. If aggregation of lists of names is possible across a single organization’s Web site/pages, that list should be evaluated on its merits and the individual aggregated elements treated accordingly. Charts and directories without names or e-mail addresses may be posted on public Web sites with position or office titles and duty phone numbers.

6.5.1.1. Individual names contained in documents posted on public Web sites may be removed or left at the discretion of the activity.

6.5.1.2. It is permissible to post names and duty information of personnel who, by the nature of their position and duties, frequently interact with the public, such as flag/general officers, PA officers, FOIA managers, or other personnel designated as official command spokespersons. Coordinate posting of such information with the FOIA or PA Office. Limit posting of biographies and photos to DOD personnel who would fit in the above category. This would include wing commanders, vice commanders, command chief master sergeants, and organizational commanders.

6.5.1.3. Use organizational/generic position e-mail addresses (e.g., office@organization.mil; helpdesk@organization.mil; commander@base.mil) for posting contact information on public sites.

6.5.1.4. Public affairs-generated products, such as press releases, are excluded from this policy.

6.5.1.5. Post directories that contain military or government advertisements or sponsorships with an appropriate disclaimer (see paragraph **5.2.2.**).

6.5.1.6. Publishing general numbers of services such as PA and other commonly requested resources on public pages is encouraged.

6.5.2. Private Web Site Information.

6.5.2.1. Names and e-mail addresses may be posted to private Web sites (restricted to .mil or .gov users) at the discretion of the local commander, when necessary to conduct official business, and after conducting the appropriate risk assessment. The risk assessment should balance the operational benefit of posting the personal information against the risk of unauthorized disclosure or alteration. The following areas should be considered in your assessment: official purpose for posting the information; possible vulnerabilities and threats to the information; the potential impact of unauthorized disclosure or modification of the information; the security of your network and existing safeguards (hardware, software, local administrative Web guidance/ policy).

6.6. Advertising. Commercial advertising and product endorsement on Air Force Web sites are prohibited (this would include advertisements contained in base/installation newspapers generated by local PA offices). However, the base may link to a publisher's Web site containing the full newspaper. Web pages that are funded with NAF resources will comply with guidance outlined in paragraph **5.2.4.**

6.7. Using Graphics and Artwork. Take great care when adapting existing artwork for use on Internet projects. Most licenses for software designed to prepare documents or briefings do not permit using the graphics for other purposes. In addition, most graphics and artwork is either copyrighted or proprietary and cannot be used without written permission from the originator or owner. Consult local legal office. Unnecessary graphics and artwork also consumes bandwidth.

6.8. Communications Bandwidth. To effectively utilize limited bandwidth, Internet users must be disciplined in the quantity and content of nonmission essential information provided via Air Force networks. Specific directions from the Deputy Secretary of Defense include:

6.8.1. Limit graphics, animation, and splash pages, etc., as much as possible, in order to reduce bandwidth usage, and to aid in response time.

6.8.2. Post large documents on the Web server instead of sending them as e-mail attachments.

6.8.3. Only download large files from Web sites when absolutely necessary.

6.8.4. Limit official subscriptions to newsgroups to the absolute minimum required to support the organization's missions and functions. Individual's personal subscriptions to newsgroups that are not mission related are prohibited unless specifically authorized by the DAA. Additionally, personal Web services such as "pointcast," or other similar "push/pull" technology may pose bandwidth and security problems, therefore, the DAA must approve access to commercial "push-pull" Web sites.

6.8.5. Imposing Web browsing restrictions may further conserve bandwidth. Accomplish this by identifying and applying good knowledge management practices such as using Intranets to post or download common use documents.

6.9. Registering a Public Site/Page. Once your organization has determined the contents of the page, following the SAF/PA format and all guidance in Title 42, U.S.C., Section 508, *Rehabilitation Act of 1998*, the process of getting the page on the Web server for your base/installation can begin. Submit a written request to your base/installation communications group or organization through the respective Web Page Maintainer.

6.9.1. Hyperlink Restrictions. You can use hyperlinks from a public Web site to other .mil/.gov public Web sites. Do not use hyperlinks from public Web sites to private Web sites, even if password-protected, for any reason.

**7. Warning Notices and Banners.** Ensure appropriate warning notices and banners (see paragraph 7.1. or 7.2.) are present on each root-level organization/function/activity home/front page, by either display, pop-up screen, or a link to the actual notice. Subordinate pages may also display or link the banner and restrictions. Add Privacy Act, RCS, and OMB statements where required.

7.1. Public Web Pages. Ensure the Notice and Consent banner is placed on each Web page. Providing a statement such as "Please read this privacy and security notice" linked to the actual notice is satisfactory. Public pages will have a Privacy and Security Notice prominently announced on the first page of all major sections of each public Web site, by either display, pop-up screen, or a link to the actual notice. All information collected must be described in this notice. Tailor public Web site banners to the audience and type of information presented. The notice further describes how, in general, security is maintained on the site, and what specific information is collected, why it is collected, and how it is used. Providing a statement such as "Please read this privacy and security notice" linked to the actual notice is satisfactory. Organizations will avoid flashy graphics or other indicators that create a misperception of danger, such as skull-and-crossbones logos or "warning" signs. Intelligence agencies must comply with the provisions of DODD 5240.1, *DOD Intelligence Activities*, April 25, 1988.

7.1.1. Comply with AFI 33-332, AFI 33-360, Volume 2, and AFI 33-324, *The Information Collections and Reports Management Program; Controlling Internal, Public, and Interagency Air Force Information Collections*, if applicable, when collecting information from the public. AFI 33-324 requires OMB approval when collecting identical information from ten or more members of the public. Such requests include surveys using check box, radio button or text form fields. Coordinate with local Forms Manager to determine if your information collecting program meets criteria of an official form.

7.1.2. AFI 33-332 directs that a Privacy Act Statement is provided when collecting personal information directly from an individual that is retrieved by name or personal identifier (i.e., SSN). Maintain this information in an approved Privacy Act system of records that is published in the

Federal Register. Inform the visitor when the information is maintained and retrieved by name or personal identifier in a system of records; that the Privacy Act gives them certain rights with respect to the government's maintenance and use of information collected about them, and provide a link to the Air Force's Privacy Act policy and system notices at **http://www.foia.af.mil**.

7.1.3. Anytime a public Web site solicits personally-identifying information, even when not maintained in a Privacy Act system of records, it requires a Privacy Advisory. The Privacy Advisory informs the individual why the information is solicited and how it will be used. Post the Privacy Advisory to the Web page where the information is being solicited, or through a well-marked hyperlink "Privacy Advisory - refer to the Privacy and Security Notice that describes why this information is collected and how it will be used."

7.1.4. Guidance on required text of the privacy and security notice for public pages follows:

7.1.4.1. The following privacy and security notice may be tailored in the indicated areas by each organization sponsoring a publicly accessible Web site. The appropriate local legal office official will approve this notice before use:

*Link from Index.html pages – "Please read this privacy and security notice."*

*( ) - indicates sections to be tailored at the base/installation level*

*[ ] - indicates hyperlinks*

** - indicates information located at the hyperlink destination indicated*

7.1.4.2. (Web site name) is provided as a public service by the ([unit or installation]).

7.1.4.3. Information presented on (Web site name) is considered public information and may be distributed or copied. Use of appropriate byline/photo/image credits is requested.

7.1.4.3.1. For site management, [information is collected]* for statistical purposes. This government computer system uses software programs to create summary statistics which are used for such purposes as assessing what information is of most and least interest, determining technical design specifications, and identifying system performance or problem areas.

7.1.4.3.2. Table 3, shown below, depicts an example of the information collected based on a standard request for a WWW document: The information below should be tailored, if necessary, to show an accurate example of the specific information being collected. * Link from above - "information is collected" to the following text:

**Table 3. Information Collected from (Defense Link) for Statistical Purposes.**

| |
|---|
| xxx.yyy.com - - [28/Jan/1997:00:00:01 -0500] "GET /Defense Link/news/nr012797.html HTTP/1.0" 200 16704 Mozilla 3.0/**http://www.altavista.digital.com** |
| **xxx.yyy.com (or 123.123.23.12)**-- this is the host name (or IP address) associated with the requester (you as the visitor). In this case, (.com) the requester is coming from a commercial address. Depending on the requester's method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via many Internet Service Providers assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) will identify a specific computer if that computer has a fixed IP address. |
| **[28/Jan/1997:00:00:01 -0500]** -- this is the date and time of the request |
| "**GET /Defense Link/news/nr012797.html HTTP/1.0**" -- this is the location of the requested file on (Defense Link) |
| **200** -- this is the status code - 200 is OK - the request was filled |
| **16704** -- this is the size of the requested file in bytes |
| **Mozilla 3.0** -- this identifies the type of browser software used to access the page, which indicates what design parameters to use in constructing the pages |
| **http://www.altavista.digital.com** - this indicates the last site the person visited, which indicates how people find (Defense Link) |
| Requests for other types of documents use similar information. *No personally-identifying information is collected.* |

7.1.4.4. For site security purposes and to ensure that this service remains available to all users, this government computer system employs software programs to monitor network traffic to identify unauthorized attempts to upload or change information, or otherwise cause damage.

7.1.4.5. Use raw data logs only to identify individual users for authorized law enforcement investigations or national security purposes. These logs are scheduled for regular destruction in accordance with the Air Force Web-RIMS RDS located at **https://webrims.amc.af.mil/rds/index.cfm**.

7.1.4.6. Unauthorized attempts to deny service, upload information, alter information, or attempt to access a non-public site from this service are strictly prohibited and may result in criminal prosecution under Title 18, U.S.C., Section 1030, *The National Information Infrastructure Protection Act*, or other applicable criminal laws.

7.1.4.7. If you have any questions or comments about the information presented here, please send them to the Web Page Maintainer.

7.1.4.8. Depending upon the requestor's method of network connection, the host name (or IP address) may or may not identify a specific computer. Connections via the many ISPs assign different IP addresses for each session, so the host name identifies only the ISP. The host name (or IP address) identifies a specific computer if the computer uses a fixed IP address.

7.1.4.9. Cookie Disclaimer (use one of the following as applicable).

7.1.4.9.1. (Web Site Name) does not use persistent cookies, i.e., tokens that pass information back and forth from your machine to the server and remain after you close your browser.

7.1.4.9.2. (Web Site name) does use session cookies, i.e., tokens that remain active only until you close your browser, in order to (make the site easier for you to use). No database of information obtained from these cookies is kept, and when you close your browser, the cookie is deleted from your computer. (Web Site name) uses cookies in the following ways: (describe use, e.g., "to save you time in filling out IMTs," "to maintain a relationship between the image and the correct link, the program that displays the banners on the bottom of some of our pages uses a session cookie"). You can choose not to accept these cookies and still use the site, but you may need to enter the same information repeatedly and clicking on the banners will not take you to the correct page. The help information in your browser software should provide you with instruction on how to disable cookies. (See paragraph **9.** for additional guidance on cookies)

7.2. Private Web Pages. Ensure the Notice and Consent banner is placed on the first page of unit's home page in accordance with AFI 33-219. Each organization/function/activity home page will display the exact banner wording found in AFI 33-219 by display, pop-up screen, or a link to the actual notice. Subordinate pages may display or link the banners. Pop-up screens are also permissible.

7.2.1. Private Web site restriction. "This site is intended for the use of the Air Force [or military, DOD, government audiences] only. Do not reproduce or distribute the content of this site to a wider audience without coordination with the information owner, your unit legal and public affairs offices."

7.3. Educational Research, Studies, and Analysis. Research, studies, and analysis done for educational purposes will post the same warning banner as the paper products. The banner should read: "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."

**8. Clearing and Releasing Information Placed on Public/Private Web Sites or Other Bulletin Boards.** Directors/deputies, chiefs of special staff agencies, commanders, or their designated representatives must review and approve for release all information destined for public Web sites. The organization's PA office must approve information destined for the public page. Once approved, updates to the Web page do not require the review process. Changes to the Web page require the Information Provider to reaccomplish the review process (**Attachment 5** and **Attachment 6**).

8.1. Public Web Sites. Public Web sites exist as part of the Air Force's public communication program and contribute to the overall image of the Air Force, increased public awareness, trust and support, airmen morale and readiness, and global influence and deterrence. "Public information" refers to information approved for "unlimited" worldwide access and distribution on the Internet. Public information has no access or security controls to limit access to the information. Because Public Web sites have global distribution, you must clear the information in accordance with AFI 35-101. Public Web sites will not contain any classification markings.

8.1.1. Approval to Establish a Public Web Site. Approval authority for establishing Public Web sites will correspond to existing authority to make public release of information (normally the wing commander or equivalent). Organizations seeking to establish a Public Web site must coordinate with local PA (and in the case of ANG units, the State PAO) and MAJCOM DAAs prior to receiving release authority (generally unit commander) approval. Only information intended for unrestricted distribution is appropriate for Public Web sites. The decision to establish such a site must weigh the value added by the site to the Air Force public image and public communication program against the maintenance costs and potential security risks.

8.1.2. Procedures for Clearing Information for Public Release.

8.1.2.1. Since the intended audience for public information is the general public, no access or security controls are necessary. However, servers must provide sufficient protection to guard against contamination or defacement of Air Force pages or unauthorized access to other parts of the Air Force system. Clearing information for public release must follow established procedures as set forth in AFI 35-101 and Internet release package (**Attachment 3**).

8.1.2.2. When reviewing information for public release, remember that the information should be of value to the general public. Do not place information of value to only military or other government agencies on Public Web pages. Coordinate with your PA offices on all information destined for public release (see paragraph **3.9.**).

8.1.3. DODD 5400.7-R/AFSUP1 requires records that an agency determines likely to be the subject of subsequent or frequent FOIA requests to be placed in a FOIA Reading Room on the public Web server. The local FOIA Office manages these reading rooms and links the site to the Air Force FOIA Web site at **http://www.foia.af.mil**. FOIA officers will coordinate with PA, legal office, and records owners to determine which frequently requested records are releasable to the public through public reading rooms.

8.1.4. Information Not Appropriate for Public Release. Under no circumstances are the following types of information allowed on Public Web sites:

8.1.4.1. Classified information (see AFI 31-401).

8.1.4.2. For Official Use Only (FOUO) information, and information that qualifies for withholding under exemptions 2 through 9 of the FOIA (see DOD 5400.7-R/AF Sup).

8.1.4.2.1. Privacy Act protected information (see AFI 33-332).

8.1.4.2.2. DOD contractor proprietary information (see AFI 61-204).

8.1.4.2.3. Scientific and Technical Information (STINFO) (see AFI 61-204).

8.1.4.2.4. Attorney-client privileged information (see AFI 51-105, *Automated Legal Information Services and Library System*).

8.1.4.3. Unclassified information requiring special handling (see AFI 33-113, *Managing Air Force Messaging Centers*).

8.1.4.4. Critical information as outlined in AFI 10-1101. Sensitive mission data that by itself is unclassified, but when combined with other available data, may reveal classified information.

8.2. Private Web Sites. Each OPR should recognize that "private information" refers to that information released on the Web with file or database access restrictions appropriate for the content. Adding safeguards will limit access to specific individuals or groups and protect the site's content. The Information Provider must determine the appropriate security and access controls required to safeguard the information (see **Table 2.**).

8.2.1. Procedures for Clearing Information for Private Web Sites. Since the Web 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 release on private Web sites, 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. Where appropriate, refer to DOD O-5200.1-I or contact the OPSEC office for assistance.

8.2.1.1. To place information on private Web sites, the Web Master and Web Page Maintainer must stay aware of the types of security and access controls available 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.

8.3. SIPRNET Web sites. Information must be appropriate for the classification level intended (see AFI 31-401). The following types of classified information may not be displayed on the SIPRNET: Top Secret, classified information carrying a Special Access Required caveat, classified information carrying a SCI caveat, classified information containing a NATO classification, classified information containing a CNWDI caveat, and information containing a Department of Energy Sigma caveat.

8.4. Document the Release Process. Before release, the Information Provider coordinates and documents the process used to review information proposed for public Web site release. Review processes may vary depending on the type and value of the information considered for release. Information Providers will maintain completed IRP until the corresponding information is removed from the Internet. The Information Provider is accountable in the event of unauthorized disclosure of private information. See **Attachment 2** for a sample IRP (**Attachment 3** for a public page sample).

8.4.1. Prepare an IRP for each unit (e.g., Squadron, Detachment, and staff equivalent). This will include all unit public Web pages.

8.4.2. Routinely updated information does not require release authority's review after initial approval unless additions or changes significantly alter the information. When the unit Web pages are significantly revised, the Web Page Maintainer updates the original IRP and regains approval. Minor changes do not require another approval.

8.5. Republishing of Base Newspapers on the Web. Base newspapers are established according to DOD Instruction (DODI) 5120.4, *DOD Newspapers, Magazines, and Civilian Enterprise Publications*, June 16, 1997, and AFI 35-101. Though generally public domain, base newspapers exist as part of the Air Force's internal information program. While the publishing of base newspapers constitutes public release of information, the distribution is limited. Public Web sites constitute global release; therefore, some information appropriate for base newspapers is not appropriate for public Web sites.

8.5.1. Reproducing the contents of base newspapers for the Web is permitted if that content meets the restrictions provided. Air Force personnel may not directly or indirectly reproduce commercial advertisements or endorsements within the newspaper when displayed on public Web sites. However, the base may link to a commercial publisher's Web site containing the full newspaper.

8.5.2. The posting of sensitive overseas and routinely deployable assignments, names, locations, and specific identifying information about family members of DOD employees and military personnel is strictly prohibited.

8.5.3. Review all stories against the *DOD Web Site Administration Policies and Procedures*, before posting to public access Web sites.

**http://www.defenselink.mil/webmasters/policy/dod_web_policy_12071998_with_amendments_and_corrections.html**

**http://www.defenselink.mil/nii/org/cio/doc/webpolicy-26april2001.html**

**9. Data Collection and Privacy Policies.** DOD Web Site Administration Policies & Procedures policy prohibits the use of Web technology that collects personally-identifying information such as extensive lists of previously visited sites, e-mail addresses, or other information to identify or build profiles on individual visitors (i.e., "persistent cookies") to DOD public Web sites.

9.1. Persistent Cookie. Persistent cookies are authorized only when the Secretary of Defense has personally approved use of the cookie, clear and conspicuous notice is given, there is a compelling need to gather the data on the site, and appropriate technical procedures have been established to safeguard the data. Send requests for approval to use persistent cookies at least 60 days prior to operational need date through the MAJCOM DAA to HQ USAF/ILC. The request will describe the need and safeguards to be used to protect the data, provide an explanation of why other technical approaches are inadequate, and include a copy of the privacy notice(s) proposed for use. HQ USAF/ILC will coordinate all waiver requests with AF-CIO/P before forwarding to the Assistant Secretary of Defense (Network and Information Integration (ASD[NII]) for Secretary of Defense approval.

9.2. DOD Web Site Administration Policies & Procedures policy, however, does permit the use of "session cookies" or other Web technology to collect or store information, but only if users are advised of what information is collected or stored. Lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency or intelligence agency of the Air Force are exempt from this policy.

**10. 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 (for mission-related purposes only) 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 or Web Page Maintainer of the replicating file server will contact the counterpart of the information to obtain written permission to replicate the information and verify that the information can be released. The information replicated is kept up-to-date by the replicating site's Web Page Maintainer or Information Provider.

## 11. Approval to Operate a Server on the Internet.

11.1. DAA Approval. All systems must receive accreditation and authorization to operate by the appropriate DAA prior to actual use (see AFI 33-202, *Network and Computer Security*). This applies to all servers directly connected to the network.

11.2. 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 and provides OPRs feedback on the usefulness of their information as well. 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.

11.3. DOD PKI Server Certificate. In accordance with Assistant Secretary of Defense, Command, Control, Communications, and Intelligence (now ASD(NII) Memorandum, subject: *"Department of Defense (DOD) Public Key Infrastructure (PKI) Update*, May 21, 2002; all private Air Force Web servers must be issued a DOD X.509 PKI Server Certificate and have 128-bit encryption Secure Sockets Layer (SSL) using this certificate enabled at all times.

## 12. Systems Security Considerations.

12.1. Internet Vulnerabilities. Without the appropriate security measures and controls, information placed on the Internet can become available to unauthorized personnel. Using access controls effectively reduces the risk of unauthorized release of information via the Internet.

12.1.1. 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. Interception of the information can occur at any point along the way. Implement security controls to prevent unauthorized disclosure of information. Any security controls implemented in the Internet must meet Federal Information Processing Standard (FIPS) 140-2, *Security Requirements for Cryptographic Module*s. To fully protect information resources, both access and security controls are required.

12.1.2. Internet Threats--Structured and Unstructured Attacks. Internet proliferation, combined with the growth of information stored, processed, or transmitted on Air Force computer systems, increases the threat and vulnerability of Air Force information resources. Network attacks come in two forms--structured and unstructured. Another threat to Air Force networks is the insider threat. For detailed threat information and preventive measures, personnel should contact their supporting Information Assurance (IA) office, the Air Force Network Operations Security Center (AFNOSC), or the Office of Special Investigations.

12.1.2.1. Structured attacks are sophisticated and organized, and are the most severe threat to Air Force systems and information resources. 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.

12.1.2.2. Unstructured attacks are less organized and may involve only a single attacker. Usually they employ the same techniques as structured attacks. For example, the common computer "hacker" is an unstructured attacker. These attackers pick their targets at random by probing different domains in search of system vulnerabilities to exploit. Hackers may infiltrate systems out of curiosity, to boost their status, or simply be destructive. Some destructive ones have malicious intentions (e.g., implanting logic bombs, Trojan horses, denial of service attacks, or altering data) just to cause damage to the system and its legitimate users.

12.1.2.3. There are two types of internal threats: deliberate and unintentional. The IA offices can provide information on the kinds of threats to look for--hints on these kinds of threats. These threats are excellent justification for frequent backups of the base/installation Web site and its related pages.

12.2. Countering the Threat. The Air Force has implemented a robust Defense in Depth program to thwart most of these threats through a program called "Information Assurance." System administrators are the first line of defense in protecting Air Force automated information systems. They work with MAJCOM NOSCs, and the AFNOSC to implement this layered approach to network defense. The AFNOSC works closely with network defenders at all levels to identify new threats and vulnerabilities and implement countermeasures. The local information assurance office provides expertise in educating systems administrators, workgroup managers, Web Masters, Web Page Maintainers, and Information Providers on current threats, vulnerabilities, and protection techniques. In a Web environment, the information providers are also essential 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, workgroup managers, Web Masters, Web Page Maintainers, and Information Providers must maintain a close working relationship with the IA 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:

12.2.1. 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). An experienced systems administrator can thwart these techniques with information and software from the IA office.

12.2.2. Packet Sniffers. Information traverses the Internet in packets through a series of computers. A packet sniffer is a program and/or device used to monitor information traveling in a packet over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. Once intruders have gained access, they can activate a program (such as a Trojan horse) to collect information traversing the computer (e.g., Internet domain, account names, identifications (ID), and passwords). Generally, good password administration and encryption techniques can thwart this threat.

12.2.3. Trojan Horse. Hidden computer viruses or viruses in disguise. Trojan horses are often computer programs embedded in other programs or software. The intruder does this so the user is unaware of the Trojan horse's presence or existence. This virus, when executed by the user, is able to spread to other programs. Some Trojan horses hide within a system and when executed, capture information (e.g., IDs and passwords of legitimate users); some damage, destroy, or steal data, while others destroy the operating system's software. In the event of a compromised ID/password, an intruder is equipped to enter the network as a legitimate user.

12.3. 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. Where 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 on the decompressed files. To prevent the possibility of rapidly spreading a virus, do not download files to a network or shared drive.

12.4. User IDs and Passwords. AFMAN 33-223 governs the use of passwords on Air Force systems.

12.5. 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 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.

12.6. 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 determination.

12.7. Operations Security (OPSEC). The Internet access available to personnel at home is an additional security factor. OPSEC training and education apply to computer use just as it does in face-to-face and phone conversations and correspondence. Policies restricting communications with unauthorized personnel also apply to Internet communications. Newsgroups (Network News Transfer Protocol [NNTP], Usenet News, Chats, etc.) give personnel the opportunity to converse electronically to a worldwide audience. Military and government employees will not discuss 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. Limiting details is an easily applied countermeasure that can decrease vulnerabilities while still conveying essential information. Follow these additional steps to eliminate improper postings: verify official need for posting, apply the OPSEC process (identify critical information, analyze threats and vulnerabilities, assess risks, and apply countermeasures), use the required clearance process, protect information according to its sensitivity, and provide training.

## 13. Information Collections, Records, Forms and Information Management Tools (IMT).

13.1. Information Collections. Annual Multi-disciplinary Review Board RCS SAF-PAS(A) 0203.)

13.2. Records. Records pertaining to IRPs, board minutes and audit control logs are created by this publication (paragraph **8.4.**). Retain and dispose of these records according to Air Force Web-RIMS RDS, Table 37-18, Rule 17, located at **https://webrims.amc.af.mil/rds/index.cfm**.

13.3. Forms or IMTs (Adopted and Prescribed).

13.3.1. Adopted Forms or IMTs: AF IMT 847, **Recommendation for Change of Publications**, AF IMT 2519**, All Purpose Checklist;** and AF IMT 3215, **IT/NSS Requirements Document**, are adopted in this publication.

13.3.2. Prescribed Forms or IMTs: No IMTs are prescribed by this publication.

DONALD J. WETEKAM, Lt Gen, USAF
DCS/Installations and Logistics

## Attachment 1

## GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

***References***

Public Law 104-13, *Paperwork Reduction Act of 1995*

Title 18, U.S.C., Section 1030, *National Information Infrastructure Protection Act*

Title 42, U.S.C., Section 508, *Rehabilitation Act of 1998*

CJCSM 6510.01, *Defense-in Depth: Information Assurance (IA) and Computer Network Defense (CND)*, 25 March 2003

DODI 5120.4, *Department of Defense Newspapers, Magazines and Civilian Enterprise Publication*s, June 16, 1997

DOD O-5200.1-I, *Index of Security Classification Guides*, September 1996, with Change 1, November 26, 1997

DOD 5200.1-R, *Information Security Program*, January 1997

DODD 5230.9, *Clearance of DOD Information for Public Releas*e, April 9, 1996; with Change 1, July 15, 1999

DODD 5240.1, *DOD Intelligence Activitie*s, April 25, 1988

DOD 5400.7-R/AFSUP 1, DOD *Freedom of Information Act Program*

DOD 5500.7-R, *Joint Ethics Regulation (JER*), August 1993, with Change 4, August 6, 1998

DODD 8500.1, *Information Assurance*, October 24, 2002

DOD Policy, *Web Site Administration Policies and Procedure*s, November 25, 1998, with amendments and corrections, updated January 11, 2002

DOD Web Site Administration Policy, July 19, 2002

FIPS 140-2, *Security Requirements for Cryptographic Modules*

Article 92, Uniform Code of Military Justice, Failure to Obey Order or Regulation

Director, Administration and Management, Washington Headquarters Services, Memorandum, *Withholding of Personally Identifying Information Under the Freedom of Information Act (FOIA)*, November 9, 2001

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

AFPD 33-2, *Information Protection* (will become Information Assurance)

AFPD 37-1, *Air Force Information Management* (will become AFPD 33-3)

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

AFI 10-1101, *Operations Security*

AFI 31-401, *Information Security Program Management*

AFI 33-103, *Requirements Development and Processing*

AFI 33-113*, Managing Air Force Messaging Centers*

AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*

AFI 33-202, *Network and Computer Security*

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

AFI 33-324*, The Information Collections and Reports Management Program, Controlling Internal Public and Interagency Air Force Information Collections*

AFI 33-332, *Air Force Privacy Act Program*

AFI 33-360, Volume 2, *Content Management Program-Information Management Tool (CMP-IMT)*

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

AFI 51-105, *Automated Legal Information Services and Library System*

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

AFI 65-106, *Appropriated Fund Support of Morale, Welfare, And Recreation (MWR) and Nonappropriated Fund Instrumentalities (NAFIS)*

AFMAN 33-223, *Identification and Authentication*

AFMAN 37-123, *Management of Records*

IEEE Standard 2001*, IEEE Recommended Practice for Internet - Web Site Engineering, Web Site Management, and Web Site Life Cycle*, 2002

AF-CIO Policy Memorandum 03-01, *Web Site Policy*, 28 January 2003

***Abbreviations and Acronyms***

**AETC**—Air Education and Training Command

**AFNOSC**—Air Force Network Operations Security Center

**AFCA**—Air Force Communications Agency

**AFI**—Air Force Instruction

**AFMAN**—Air Force Manual

**AFPD**—Air Force Policy Directive

**AFRC**—Air Force Reserve Command

**ANG**—Air National Guard

**ASD (NII)**—Assistant Secretary of Defense (Networks and Information Integration)

**CNWDI**—Critical Nuclear Weapons Design Information

**CSO**—Communications and Information Systems Officer

**DAA**—Designated Approving Authority

**DISN**—Defense Information Systems Network

**DOD**—Department of Defense

**DODD**—Department of Defense Directive

**DRU**—Direct Reporting Unit

**DSAWG**—DISN Security Accreditation Working Group

**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

**GIG**—Global Information Grid

**GILS**—Government Information Locator Service

**HTML**—Hypertext Markup Language

**HTTP**—Hypertext Transfer Protocol

**IA**—Information Assurance

**ID**—Identification

**IEEE**—Institute of Electrical and Electronics Engineers

**IMT**—Information Management Tool

**IP**—Internet Protocol

**IRP**—Internet Release Package

**ISP**—Internet Service Provider

**MAJCOM**—Major Command

**MWR**—Morale, Welfare, and Recreation

**NAF**—Nonappropriated Funds

**NATO**—North Atlantic Treaty Organization

**NCC**—Network Control Center

**NIPRNET**—Non-Secure Internet Protocol Router Network

**NNTP**—Network News Transfer Protocol

**NOSC**—Network Operations Security Center

**OMB**—Office of Management and Budget

**OPR**—Office of Primary Responsibility

**OPSEC**—Operations Security

**PA**—Public Affairs

**PAO**—Public Affairs Officer

**PAS**—Privacy Act Statement

**POC**—Point of Contact

**PKI**—Public Key Infrastructure

**QoL**—Quality-of-Life

**RCS**—Report Control Symbol

**RDS**—Records Disposition Schedule

**SAF**—Secretary of the Air Force

**SCI**—Sensitive Compartmented Information

**SIPRNET**—Secret Internet Protocol Router Network

**SSN**—Social Security Number

**SSL**—Secure Sockets Layer

**STINFO**—Scientific and Technical Information

**TCP/IP**—Transmission Control Protocol/Internet Protocol

**UCMJ**—Uniform Code of Military Justice

**URL**—Uniform Resource Locator

**USAF**—United States Air Force

**USAFA**—United States Air Force Academy

**USERID**—User Identification

**WWW**—World Wide Web

***Terms***

**Air Force Link**—The official Web information service for the Air Force (**http://www.af.mil/**).

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

**Client**—In networking, a software application that allows the user to access a service from a server computer (e.g., a server computer on the Internet).

**Cookie**—In Web browsing, a small text file, called cookie.txt, that is generated by the Web site and stored on the user's computer hard disk, ready for future access. On subsequent visits to the Web site, the Web site reads the cookie from the user's hard disk. Cookies can be used for a variety of purposes, such as to recording log-on information, revealing the user's shopping preferences, Web sites visited, etc. Cookies can also provide Web sites with personal information about the user from information stored on the user's hard drive. Also called first-party cookie.

**Communications and Information Systems Officer (CSO)**—The officer responsible for communications and information systems and functions at any Air Force organizational level. At base level, the "base CSO" is the commander of the communications unit responsible for carrying out base systems duties, including management of the basewide C4 infrastructure. At the MAJCOM level, the

"MAJCOM CSO" is designated by the MAJCOM commander and is responsible for the overall management of the MAJCOMs communications and information assets.

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

**Extranet**—The private access page aimed towards audiences outside the unit/organization.

**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.

**Government Information Locator Service (GILS)**—An effort to identify, locate, and describe publicly available Federal information resources, including electronic information resources. GILS records identify public information resources within the Federal Government, describe the information available in these resources, and assist in obtaining the information. GILS is a decentralized collection of agency-based information locators using network technology and international standards to direct users to relevant information resources within the Federal Government.

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

**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. Also referred to as a "link."

**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 language used to create WWW pages, with hyperlinks and markup for text formatting (different heading styles, bold, italic, numbered lists, insertion of images, etc.).

**Hypertext Transfer Protocol (HTTP)**—The protocol most often used to transfer information from WWW servers to browsers.

**Information Provider**—The person or organization that provides information for posting on a Web Page and is responsible for the content, coordination, and classification of that information.

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

**Internet**—An informal global collection of government, military, commercial, and educational computer networks. 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 private network that works like the Web, but is not on it. Usually owned and managed by an organization, an Intranet enables an activity to share its resources with its employees without sensitive information available to everyone with Internet access. Intranets may allow connection outside the Intranet to the Internet through firewall servers and other security devices that have the ability to screen messages in both directions to maintain the organization's security.

**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 the 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. Foil spoofing by using a filtering router that drops "outside" packets with an "inside" source address.

**Link**—Used interchangeably with hyperlink.

**Military Controlled Access Paths**—Unclassified networks or "links" that are leased, configured, managed, and secured by a government agency. This includes the NIPRNET-Air Force as well as dedicated links that have a node on the base network.

**Mobile Code**—Software modules obtained from remote systems, transferred across a network, and then downloaded and executed on local systems without explicit installation or execution by the recipient.

**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.

**Personally-Identifying Information**—Information that includes, but is not limited to: name, e-mail. IP address, postal address, and/or telephone number, that can be used to identify an individual.

**PKI Certificate**—A digital representation of information that binds the user's identification with the user's public key in a trusted manner. At a minimum, this information (1) identifies the certification authority issuing it, (2) names or identifies its user, (3) contains the user's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.

**Private Information**—Applies to information approved for a limited audience. This information has added safeguards that restrict access to a specific group or groups. The Information Provider must determine the appropriate security and access controls required to safeguard the information.

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

**Private Web Server**—A Web server designed for and/or provides information resources limited to a particular audience (i.e., DOD) or a subset thereof. (This includes Web servers that provide interfaces to e-mail systems.) A private Web server restricts or attempts to restrict general public access to it. The means of restriction are userid and/or password authentication, encryption (i.e., PKI certificates), and physical isolation. Consider any DOD operated Web server that provides any information resources not intended for the general public a private Web server and subject to this policy.

**Proxy Server**—A server that acts as a bridge to the Internet through which all incoming and outgoing requests go through. Used to enhance security, access control and increase performance/efficiency. A server that provides access to files from other servers by retrieving them either from its local cache or from the remote server.

**Public Information**—Information approved for unlimited public release. Public 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 Information Provider.

**Public Pages**—Web pages intended for viewing by the general public.

**Scientific and Technical Information (STINFO)**—Includes all technical publications and documents generated by all Air Force-funded research development, test, and evaluation 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, photographs, technical orders, databases, and any other information that is of usable or adaptable design to, 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 protocol from Netscape Communications Corporation, which is designed to provide secure communications on the Internet.

**Server**—A hardware platform (computer) that houses software providing service to other computers or programs to satisfy client requests and needs.

**Third-Party Cookies**—In Web browsing, a cookie generated by a Web site other than the one the user is viewing, such as an advertiser that is present at the Web site being viewed.

**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 the two 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. TCP (the "transmission control protocol") is responsible for breaking up the message into datagrams, reassembling them at the other end, resending anything that is 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.

**Unauthorized Web Site**—An Internet Web site to which access through the use of US government-owned computers and/or networks is prohibited by US law or by DOD and Air Force directives.

**Uniform Resource Locators (URL)**—(formerly Universal Resource Locator)—An Internet address which tells a browser where to find an Internet resource. For example, the URL for Computer User is **http://www.computeruser.com/**.

**Web Browser**—Software that acts as an interface between the client and the Internet, 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 Master**—The person(s) or team responsible for developing the overall corporate structure, business rules, operation, and maintenance of Web pages contained within their site structure, according to all applicable laws and instructions.

**Web Page**—One page of a document on the World Wide Web. A Web page is usually a file written in HTML, stored on a server. A Web page usually has links to other Web pages. Each Web page has its own address called a Uniform Resource Locator (URL), in the form **http://www.computeruser.com**.

**Web Page Maintainer—**The creator and/or focal point for the organization's Web pages.

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

**Web Server Administrator—**The person(s) or team who provides the system administration, maintenance, configuration management, security, and back up and recovery for Web servers.

**Web Site—**A server computer that makes documents available on the World Wide Web. Each Web site is identified by a hostname.

**Workgroup Manager (WM)—**The persons certified and appointed under AFI 33-115, Volume 2, *Licensing Network Users and Certifying Network Professionals*, that are the unit focal points for communications and information activities and provide technical and information management support to their respective units/offices.

**World Wide Web (WWW) or Web—**The subset of the Internet capable of providing the public with user-friendly graphics-based multimedia access to information on the Internet. It is the most popular means for storing and linking Internet-based information in all multi-media formats. Navigation is accomplished through a set of linked documents that may reside on the same computer or on computers located almost anywhere else in the world. It 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

## SAMPLE FORMAT FOR INTERNET RELEASE PACKAGE (IRP) AND SAMPLE FORMAT FOR PRIVATE WEB PAGE COORDINATION/APPROVAL CHECKLIST

**Page Title:**

**Date:**

**Section I:** Web page must meet the following requirements for posting information on private Web pages: (If No, explain on reverse)

1. Comply with copyright restrictions. (**2.2.5.**) (**6.7.**)

2. Contain accurate/current information. (**3.14.5.**) (**3.15.2.**) (**6.**)

3. Links are recently validated. (**3.14.3.**) (**5.2.1.**) (**6.1.1.3.**) (**6.3.1.5.**-SIPRNET)

4. Proper access and security controls are in place and operational. (**3.12.1.**) (**5.1.2.**) (**7.2.**) (**12.1.1.**) (**12.6.**)

5. Pages are not used to promote personal/commercial gain, or endorse commercial products or service. (**5.2.2.**) (**5.2.3.**) (**6.6.**) (**8.5.1.**)

6. Pages do not contain, link to, or promote obscene/offensive material. (**2.2.3.**)

7. Pages do not store/process classified material or critical indicator on nonapproved systems. (**2.2.4.**)

8. Pages do not violate vendors' license agreements. (**2.2.10.**) (**6.7.**)

9. Pages are not copies of other sources on the Internet. (**10.**)

10. Pages do not display incomplete paths or "Under Construction" pages. (**3.13.2.**) (**6.**)

11. Each page displays required warning notices and banners. (**6.1.2.2.**) (**7.2.**)

12. The top-level page contains Web Page Maintainer's organization, office symbol, commercial telephone number, DSN phone number, organizational e-mail address, and meets the minimum requirements. (**6.1.**)

13. Privacy Act and For Official Use Only information password and ID protected. (**Table 2.**). If names and/or e-mail addresses are posted, has the local commander authorized posting and risk assessment been accomplished?

14. If applicable, is DOD contractor proprietary information password and ID protected? (**Table 1.**)

15. Critical information (sensitive mission data that by itself is unclassified, but when combined with other available data, may reveal classified information) is not displayed or linked on this page. The information has been reviewed for OPSEC releasability. (**8.1.4.4.**)

16. Complies with Privacy Act requirements. Do not post personal information on Private Web pages unless it is mission essential, falls under one of the Privacy Act exceptions for disclosing to third parties without consent of the subject, and appropriate safeguards are established. Add appropriate Privacy Act Statements or Privacy Advisories to pages that collect personally-identifying information and personal information from the subject (individual) that is filed in a Privacy Act system of record. (**3.15.3.**)

17. Does the Web site/page comply with Title 42, U.S.C., Section 508, *Rehabilitation Act of 1998*? The standards may be obtained from the official Section 508 Web site at **http://www.section508.gov**. (**3.12.8.**) (**3.14.8.**)

**Section II:** This certifies that this Web page complies with AFI 33-129.

**Signature:** ______________________

**Date:** ___________________________

Web Page Maintainer: ______________________________________________

Information Provider: ______________________________________________

Unit OPSEC Monitor: ______________________________________________

Privacy Act Manager: _____________________________________________

Base Contracting (if applicable): ______________________________________

Foreign Disclosure Office (if applicable): __________________________________

Base/Unit Staff Judge Advocate (if applicable): ______________________________

Unit Commander (approval authority): ______________________________

Web Master: ____________________________________________________

## Attachment 3

## SAMPLE FORMAT FOR PUBLIC WEB PAGE COORDINATION/APPROVAL CHECKLIST

**Page Title:**

**Date:**

**Section I:** Take extreme care when considering information for release onto publicly accessible sites. Owners and/or releasers of information proposed for such release must ensure that it is not susceptible to compilation with other information to render sensitive or even classified data in the aggregate. Assess the search and data mining capabilities of Web technology from a risk management perspective. If there are any doubts, do not release the information! Web pages must meet the following requirements for posting information on public access pages: (If No, explain on reverse)

1. Comply with copyright restrictions. (**2.2.5.**) (**6.7.**)

2. Contain accurate/current information. (**3.14.5.**) (**3.15.2.**) (**6.**)

3. Links are recently validated. (**3.14.3.**) (**5.2.1.**) (**6.2.1.4.**)

4. Proper access and security controls are in place and operational. (**3.12.1.**) (**7.1.**) (**8.1.**) (**12.1.1.**) (**12.6.**)

5. Pages are not used to promote personal/commercial gain, or endorse commercial products or service. (**5.2.2.**) (**5.2.3.**) (**6.6.**) (**8.5.1.**)

6. Pages do not contain, link to, or promote obscene/offensive material. (**2.2.3.**)

7. Pages do not store/process classified material or critical indicator on nonapproved systems. (**2.2.4.**)

8. Pages do not violate vendors' license agreements. (**2.2.10.**) (**6.7.**)

9. Pages are not copies of other sources on the Internet. (**10.**)

10. Pages do not display incomplete paths or "Under Construction" pages. (**3.13.2.**) (**6.**)

11. Each home page displays required warning notices and banners. (**6.2.2.3.**) (**7.1.**)

12. Each unit or organizational top-level page contains organization name and shield, organization office symbol, commercial telephone number, organizational e-mail address, and meets the minimum requirements. (**6.2.**)

13. Pages do not provide a list of names and/or individual e-mail addresses that are exempt from release under the FOIA. (***NOTE***: One e-mail address required for legitimate inquiries or page maintenance is acceptable; however organizational/generic e-mail addresses for this use are encouraged). (**6.5.**)

14. Pages do not contain information that has value to only military and government agencies. (**8.1.2.2.**)

15. Pages do not contain hyperlinks to information outside functional area Web Page Maintainer's mission. (**5.2.1.**) (**5.2.2.4.**)

16. Pages do not contain links to or reference private access Web pages. (**6.9.1.**)

17. Pages comply with the Privacy Act and include Privacy Act statements and Privacy advisories when soliciting information from individuals? Public pages do not contain personal information unless clearly authorized by law and AFI 33-332. (**3.8.8.**) (**3.9.1.2.**) (**3.15.3.**) (**7.1.1.**) (**7.1.2.**) (**7.1.3.**) (**8.1.4.2.1.**)

18. Does the Privacy and Security notice include cookie disclaimer? No persistent or third party cookies used? (3.8.8.8) (**7.1.4.9.**) (**9.**)

19. Pages do not contain FOUO information (information exempt from release under the FOIA according to DOD 5400.7R/AF Supplement 1? (**3.8.7.**) (**8.1.4.2.**)

20. Pages do not contain DOD contractor proprietary information. (**8.1.4.2.2.**)

21. Pages do not contain Unclassified Scientific and Technical Information private by AFI 61-204. (**8.1.4.2.3.**)

22. Pages do not contain unclassified information requiring special handling according to AFI 33-113. (**8.1.4.3.**)

23. Ensure pages do not contain AFI 10-1101 critical information (sensitive mission data that by itself is unclassified, but when combined with other available data, may reveal classified information). (**8.1.4.4.**)

24. Ensure pages do not contain any classification or markings. (**8.1.**)

25. Does the Web site/page comply with Title 42, U.S.C., Section 508, *Rehabilitation Act of 1998*? The standards may be obtained from the official Section 508 Web site at **http://www.section508.gov**. (**3.12.8.**) (**3.14.8.**) (**6.9.**)

26. Ensure the Notice and Consent banner is placed on each Web page.

**Section II:** This certifies that this Web page complies with AFI 33-129.

**Signature: ________________________**

**Date ______________________________**

Web Page Maintainer: ___________________________________________________________________

Information Provider: ____________________________________________________________________

Unit OPSEC Monitor: __________________________________________________________________

Freedom of Information Act/Privacy Act Manager: _____________________________________________

Staff Judge Advocate (if applicable): _______________________________________________________

Foreign Disclosure Office (if applicable): ___________________________________________________

Base Contracting (if applicable): ____________________________________________________________

Public Affairs Representative: ______________________________________________________________

Unit Commander (approval authority): ______________________________________________________

Web Master: _____________________________________________________________________________

## Attachment 4

## SAMPLE APPOINTMENT LETTER UNIT/ORGANIZATIONAL LETTERHEAD

**Date**

**FROM:** Unit/Organizational Commander (Web Master)
2 or 3 letter directorate/division chief (Web Page Maintainer)

**TO:** Base/Installation

**SUBJ:** Appointment Letter

1. The following named personnel are appointed (Web Master or Web Page Maintainer) to perform the duties of this position.

| | **NAME** | **RANK** | **OFFICE SYM** | **DUTY PHONE** |
|---|---|---|---|---|
| **Primary** | | | | |
| **Alternate** | | | | |

2. The above named personnel have received the technical training required for the position. (Ref: AFI 33-129, *Web Management and Internet Use*)

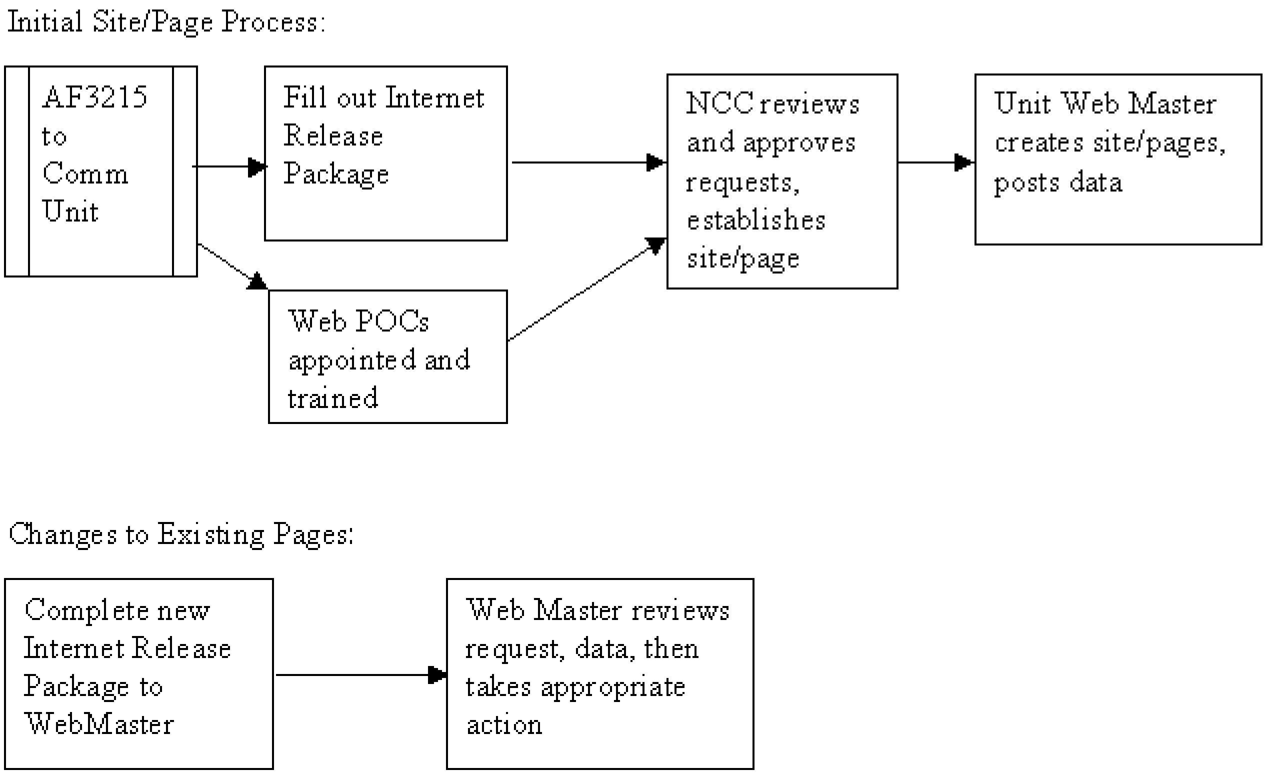
Signature block
Unit/organization

**Attachments:** training certificates (subject matter, security)

## Attachment 5

## INTERNET RELEASE PROCESS FLOW CHART

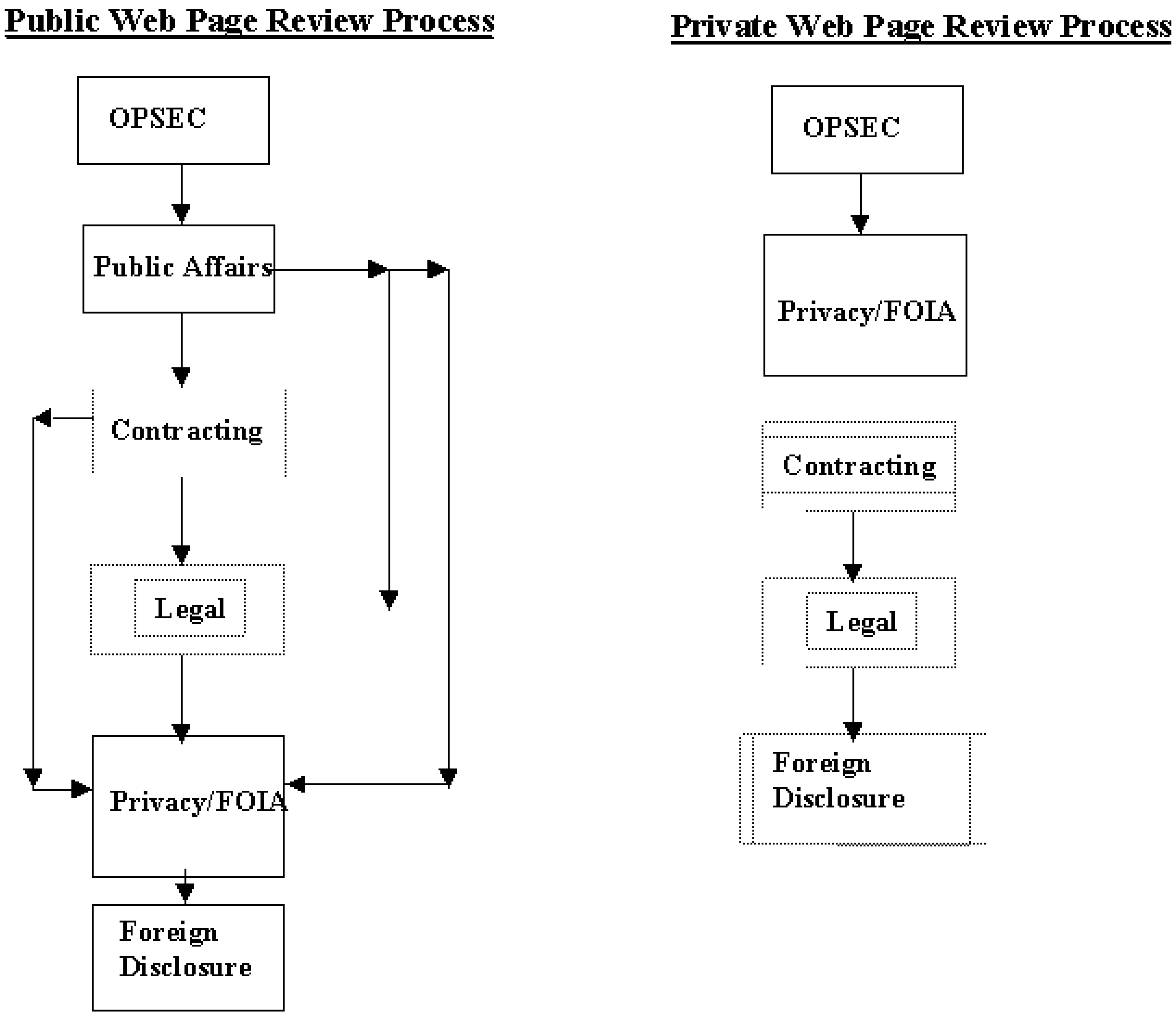
**Figure A5.1. Internet Release Process Flow Chart.**


Initial Site/Page Process:
AF3215 to Comm Unit
Fill out Internet Release Package
Web POCs appointed and trained
NCC reviews and approves requests, establishes site/page
Unit Web Master creates site/pages, posts data
Changes to Existing Pages:
Complete new Internet Release Package to WebMaster
Web Master reviews request, data, then takes appropriate action

## Attachment 6

## PUBLIC/PRIVATE PAGE REVIEW PROCESS FLOWCHART

**Figure A6.1. Public/Private Page Review Process Flowchart.**



Optional review based on information