

2 JANUARY 1998

Communications



**INFORMATION SHARING THROUGH THE
WORLD WIDE WEB**

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

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

OPR: SCMA (Major Edward J. Burbol)
Supersedes AFSPCI33-103, 24 June 1996.

Certified by: SCM (Colonel Dennis J. Rensel)
Pages: 14
Distribution: F

This instruction implements AFPD33-1, 17 Sep 93, and provides policy for accessing and disseminating information over the Internet on the World Wide Web (Web). This instruction addresses responsibilities, information content, access and protection controls, home page presentations, and outlines procedures for properly placing and maintaining information on the Web. It applies to Headquarters Air Force Space Command (HQ AFSPC) and all of its units. This instruction does not apply to the Air Force Reserve nor Air National Guard components.

SUMMARY OF REVISIONS

The revision of this publication is to meet the format standards required by Air Force. No content material has changed. Some required format changes have been made to allow for the conversion process.

1. Glossary of References and Web Terms. See [Attachment 1](#).

2. General. The Internet and World Wide Web provide an ability for us to use information physically located around the world. The World Wide Web links the computers of government, education, industry and private individuals together forming a “web” of available links to information. Like any powerful tool, we must learn to get the most out of the Internet and World Wide Web without compromising the security of our operations. This instruction establishes the policy and guidelines for obtaining information from the Web or posting information to the Web. Section A, Web Process, will help you determine what you can and can’t read from or write to the Web and describes the process you need to follow to write (or post) information to the Web. Section B, Web Responsibilities, defines duties associated with the Web. Finally, Section C, Web Administration, describes the requirements for properly securing information placed on the Web and defines the coordination required to minimize risk.

3. Categories of Web Information. Information on the Web is divided into “pages,” named as such because in viewing information on the web, it looks similar to a page in a book. While we can post almost anything which we can write or publish, this instruction concentrates on five major categories of information.

3.1. Public Access. This information is public in nature and available worldwide to everyone who has web access. This can be an invaluable tool for anyone who needs general information on topics ranging from public announcements to public relations, but remember that anyone in the world can see these pages which represent the official position of the United States Air Force.

3.2. Government and Contractor Restricted Information. Many topics that we handle in the government are not classified, but do attract a lot of attention. This restriction simply limits the number of people who have access to the information but still allows exchange of information between government agencies as well the contractors working for these agencies.

3.3. Information Limited to Base Population. We consider much of the information we work with in the military sensitive-but-unclassified. Because the Web is open to people Worldwide, we need to pay particular attention to information in this category to ensure we secure it properly. The easiest method would be to limit the posting of this type of information. This would be impractical, but there are protection measures (or firewalls) which we can install on a base network to help ensure that only people on the base are accessing this category of information. Unfortunately there are few tools available which allow multiple bases to access this type of information, so intra-base information sharing of sensitive but unclassified information may not be available for a few years.

3.4. Password Limited Information. This category of information is the most secure form of sensitive but unclassified information on the Web. We use firewalls, which are hardware barriers to unwanted electronic traffic, as well as passwords to ensure that only specified people access our servers and sites.

3.5. Classified Information. The Internet and Worldwide Web are unclassified networks. Never place classified information on either of these systems.

WARNING: Do not consider any level of protection “safe” for Web pages. Firewalls, passwords and data encryption provide a reasonable protection, but all are vulnerable. Never place classified information on the Web or information which if released, could pose a serious threat to mission sustainment or effectiveness.

4. Process for Posting to the Web:

4.1. If you would like to post a page or series of pages to the Web, start by filling out an AFSPC Form 12, World Wide Web Page Request. This form asks all of the pertinent questions your Web Master will need to post the page. Your LAN help desk will help you design the page and make it ready for publishing. After you design this page, you must obtain approval from the applicable organizations listed in **Table 1**. Note that if the public will have access to this page, your local Public Affairs must coordinate on the package. Finally, return the completed and coordinated form to your LAN help desk for posting to the Web.

4.2. Your local Web Master is the person responsible for posting information to the Web. Web Masters require an AFSPC Form 12, World Wide Web Page Request, signed by the appropriate approving official before posting pages public or limited access web servers. The Web Master keeps this form throughout the entire period of the page display.

5. Release and Approving Authorities:

5.1. Before posting a page to the Web, the person requesting the page must obtain written approval from the appropriate offices, listed in **Table 1**, before posting information to the Web. Additionally, you should consult all existing policies pertaining to the content of information involved. Contact your Base Information Security Officer for approval of all information types not listed in **Table 1**.

Table 1. Information Types and Approval Authorities.

If the Information is	then the Gov- erning Publi- cation is	and you must ob- tain approval from	Minimum Access / Transmission Con- trol
Unclassified Scientific and Technical Information (STINFO)			
Distribution A (For Public Release)	AFPD61-2	STINFO Officer & Public Affairs	Unlimited Distribution Unencrypted Trans- mission
Distribution Statement B-F	AFI61-204 (Attach 2)	STINFO Officer	STINFO Officers must determine risk and approve access controls
OPSEC	AFI10-1101	<i>See Note 2 Below</i>	protected by firewall Encrypted Transmis- sion
Foreign Disclosure	AFI16-201	<i>See Note 3 Below</i>	Password & ID Encrypted Transmis- sion
Security Awareness, Training and Education Information	AFI33-204	Security Manager & Public Affairs	Unlimited Distribution Unencrypted Trans- mission
Marked "For Official Use Only" (FOUO) Non-Privacy Act.	AFI37-131, para 26	FOIA Manager <i>See Note 1 Below</i>	protected by firewall Encrypted Transmis- sion
Freedom of Information Act (FOIA) Exempt Information	AFI37-131, para 10	FOIA Manager	.mil or .gov IP Only Encrypted Transmis- sion
Privacy Act	AFI37-132	Privacy Act Officer	Password & ID protected by firewall Encrypted Transmis- sion
Copyrighted Publications and Software	AFI51-303	Staff Judge Advo- cate	Password & ID Encrypted Transmis- sion
DoD Contractor Proprietary Information	AFI61-204	Contracting Officer	Password & ID protected by firewall Encrypted Transmis- sion
UNCLAS Publications	AFIND02	Publication Man- agement & Public Affairs	Unlimited Unencrypted Trans- mission

UNCLAS Organizational Specific Information	wing OIs	Group CC or HQ 3- Ltr	.mil or .gov IP Only
--	----------	-----------------------	----------------------

NOTES:

1. FOUO information is an extremely broad category. The review process should include the functional areas corresponding to the content of the information itself. If the value of the information is still unclear, then the information SHOULD NOT be Internet accessible. When in doubt, do not put it on the Web!
2. If the possibility of information becoming sensitive when aggregated with other unsensitive information exists, the OPR(s) should consult the Security Classification Guide and/or Operations Security Officer for assistance.
3. You may not release certain types of information, though unclassified to foreign nationals, foreign governments, foreign contractors or foreign organizations. Please consult your Foreign Disclosure Office or HQ AFSPC/XPI for information on National Disclosure Policy

5.2. Publicly Releasable Information. The appropriate HQ AFSPC, NAF or wing Public Affairs office will approve Web information requiring no access nor protection controls.

5.3. Information Not for Public Access. The functional directorate at HQ AFSPC or the appropriate NAF or wing commander approves Web information not intended for public access (see paragraphs **3.3.** and **3.4.**).

5.4. Foreign Disclosure. Foreign disclosure is primarily concerned with the following types of information: Unclassified information which requires special handling, i.e. encrypt for transmission only, scientific and technical information, controlled unclassified information, unclassified - sensitive information, technical data, AFSPC foreign disclosure policy information, AFSPC international policy information, AFSPC foreign base information, combined military information, and limited distribution information. For additional information, see AFI61-201 and AFI16-204.

5.5. Pages Under Development . The base Designated Approval Authority (DAA) will establish local procedures for posting files to servers with limited, controlled access while developing pages. These procedures must ensure that only authorized personnel see this information.

5.6. Charging for Web Information. The Paperwork Reduction Act of 1995 outlines the means of charging the public for hardcopy and electronic information. Commercial sites may reference your Web pages without cost, as long as the page is available to the public.

6. Formats for Web Pages. This instruction provides formats for Web pages in order to ensure AFSPC maintains a consistently professional look while ensuring information is useful and easy to find.

6.1. Top Level HQ AFSPC and Wing Web Pages. The home page is the top level Web page which provides an index or table of contents to linked information. AFSPC uses two types of home pages, an organizational home page and a base home page, generated and maintained by each host AFSPC wing PA office. HQ AFSPC functional offices and direct reporting units should use the same format to develop their organizational home page. HQ AFSPC/PA provides an AFSPCLink home page service, much like that used by the DoD and USAF to help their customers search for information. **Attachment 2** and **Attachment 3** show requirements for AFSPC home page formats and points to

sample templates which you can use for ease of creation and standardization. This instruction defines only the formats required for these top level indexes (home pages). Wings and HQ Directorates may provide additional guidance for page formats linked below this level.

6.2. Single Source of Information. All Web pages will identify a single office of primary responsibility to keep information on that page current. When maintaining a page, avoid copying files from other sources to place on a home page. Instead establish a link from your home page to the desired information. For example, the Air Force News Center, Kelly AFB TX, is responsible for all weapon system fact sheets and general officer biographies. Should any AFSPC unit elect to offer one of these fact sheets on their home page, they should simply refer or point to the AFNEWS home page. This ensures timely update of information at a single location and retains currency at all levels.

6.3. HyperText Links. The AFSPCLink home page will maintain hypertext links to Air Force-Link and DoD-Link home pages. AFSPC units should establish hypertext links to AFSPC's home page. Only establish hypertext links to home pages of non-government Web servers when information maintained at those sites adds value to the government. Wing pages can maintain additional links but wing procedures should include a proactive means of ensuring that all links are accurate and up to date.

6.4. Government Warning. Place the following statement on all AFSPC home pages:

WARNING!!!

UNCLASSIFIED, NON-SENSITIVE, NON-PRIVACY ACT USE ONLY!!!

Do not discuss, enter, transfer, process, or transmit classified/sensitive national security information of greater sensitivity than that for which this system is authorized. Use of this system constitutes consent to security testing and monitoring. Unauthorized use could result in criminal prosecution.

7. Responsibilities:

7.1. Public Affairs:

7.1.1. HQ AFSPC/PA provides policy and guidance to AFSPC units on publicly releasable information.

7.1.2. HQ AFSPC, NAF or wing Public Affairs approves all information for public release.

7.1.3. The Public Affairs office for each NAF, wing and direct reporting unit of AFSPC designs, implements and maintains a Web organizational home page (**Attachment 2**), and a base home page (**Attachment 3**) for host wings. Those without this capability may forward their information to the AFSPC CSS/SCNL for implementation. Headquarters, NAF or wing Public Affairs offices approves all information found on these home pages.

7.2. Communications and Information Units:

7.2.1. HQ AFSPC/SCM provides policy and guidance to AFSPC units on the physical implementation and protection of information posted on the Web.

7.2.2. Headquarters and base communications units provide technical expertise required to implement Web services, and employs appropriate access controls where necessary. Each base communications unit shall appoint a single point of contact, to be the Web Master, responsible for disseminating guidance to all Web users, while ensuring standardization of Web pages.

7.2.3. AFSPC CSS/SCNL and base LAN administrators periodically audit Web pages and usage to ensure that users are adhering to proper configuration and are accessing the Web for official business only.

7.2.4. AFSPC CSS/SCNL provides technical advice for the implementation of Headquarters, NAF or wing home pages.

7.3. Approving Officials. HQ AFSPC Directorates, NAF and wing commanders approve the posting of Web information, under their jurisdiction, not meant for public access (paragraph 3.1.). In order to ensure proper accountability, do not delegate this approval authority below the Squadron Commander level (O-5 or higher). We encourage commanders to define supplements to this policy providing further NAF or wing guidance on the processes, procedures and formats for Web implementation.

7.3.1. Value Added Versus Risk. Approving officials must compare the risks associated with disseminating information through the Internet versus the expected gain. The approving official should also assess the potential damage unauthorized disclosure can cause. Once the approving official has studied these factors and determines the risk is acceptable, then he or she should approve the information for release. The approving official is accountable for all information posted to their Internet or Web sites.

7.3.2. Value Added Versus Server Traffic. Approving officials must assess the amount of traffic that each Web page will add to the server and local area network. Weight against the value added by the information. The base communications unit is usually best equipped to make technical assessments of server and network capacity. Web Masters should inform Page owners of either minimal page usage or unusually heavy traffic patterns, so the individual updating the page can make informed posting decisions.

7.4. Web Masters. The Web Master is responsible for ensuring that each web page under his or her control is: properly secured, professionally presented, current, accurate, factual, and related to AFSPC's mission. Additional responsibilities of the Web Master include:

7.4.1. Ensuring all information under their control has been properly reviewed and documented before being placing on the Web

7.4.2. Ensuring all links under their control comply with Air Force and AFSPC policies and are in place and operational

7.4.3. Ensuring proper access and protection controls are in place and operational.

7.4.4. Ensuring usernames and passwords are valid and up-to-date.

7.4.5. Ensuring information which is outdated or superseded is removed from the system.

7.4.6. Following local procedures to work with other page owners to minimize the risk of increased information sensitivity associated with the aggregation of unclassified information.

7.4.7. Meeting periodically with other Wing and HQ AFSPC Web Masters for crossfeed, process evaluation and information protection training.

7.4.8. Registering the Web site. The Web Master will register all Web sites residing on Air Force systems, contracted using Air Force resources, or Air Force sponsored, using the process described at Uniform Resource Locator (URL) "http://www.af.mil/sites." The purpose of regis-

tration is to develop the Government Information Locator Service (GILS), an initiative of AF/SCXX, SAF/PAR.

7.5. User:

7.5.1. All resources required to implement Web pages to include additional software, hardware, and connectivity are the responsibility of the requiring organization.

7.5.2. Access to the Internet through a government computer or network is governed by the Standards of Ethical Conduct (5 CFR 2635.704), the Joint Ethics Regulation (DoD 5500.7-R) and as further specified below. Viewing, downloading, copying, sending, posting or processing information via the Web when not in the conduct of official business are activities strictly prohibited and may result in administrative, non-judicial, or judicial punishment for civilian or military personnel.

8. Protection Considerations:

8.1. Internet Vulnerabilities. Since the Internet is a public network with limited access controls, information made available on the Web is basically available to anyone. Information owners can limit (with a certain level of risk) user access to their information through the use of firewalls, access controls, passwords, and data encryption.

8.2. Information retrieved over the Internet. To minimize the rapid spread of viruses, do not download files to network or shared drives. Check all files for viruses after downloading using local DAA approved procedures. HQ AFSPC, NAF or wing base communications unit must approve all executable program files before use.

8.3. Server Protection. All servers connected to the Internet must have formal DAA authorization to operate in accordance with DoD 5200.28 and AAFP33-2.

8.4. Barrier Zones. With the various types of information available to users of the Internet, we must protect our servers and information appropriately. This instruction defines four zones. A base may choose to use any combination of these zones based on their protection requirements and expected use. Connect each zone to its own server. Partitioning servers can not guarantee the “multi-level” protection required.

8.4.1. Zone 1 - Publicly Releasable Information. This server set up allows the public to view any of the information available on that server. This server has minimal viewing restrictions and need not be under the protection of a firewall. The base (or higher) Public Affairs must approve all information placed on this server. Examples of this type of information include the wing home page and the base home page.

8.4.2. Zone 2 - Traffic Restriction. This server allows the base to reduce traffic coming into a server by allowing only specific domains or IP addresses through the use of routers and filters. Do not place FOUO, to include Privacy Act, information on this server. Usually, restrictions include “just military, government or military contractors” (.mil or .gov domains). Public Affairs does not need to approve information on this server but the approving official (at the O-5 level) must approve the AFSPC Form 12. Note that this traffic restriction zone can be “spoofed” but not by your “every day” hackers. Information on this server must be unclassified, non-FOUO, non-sensitive information only and only disseminated to authorized personnel.

8.4.3. Zone 3 - Firewall Protected FOUO. A firewall or set of routers and firewalls protects this server. This zone is cleared for certain types of FOUO. See **Table 1.** for minimum protection and transmission requirements. System administrators will place information on this server after obtaining approval from the O-5 approving official (paragraph **3.2.**, **3.3.**). Public Affairs approval is not required for information posted behind the protection of this firewall.

8.4.4. Zone 4 - Firewall and Password Protected FOUO. A firewall and a set of passwords protects this server. Use this server when positive identification of people and the machines that they are using is required for FOUO information.

8.5. Password Restrictions. Passwords transmitted over the Internet must be unique, one time passwords, and/or, encrypted, to prevent interception by unauthorized individuals. Administrators should restrict passwords to random combinations of at least six alphanumeric and/or symbol characters that are not dates, names, phone numbers, social security numbers, or words. Software is available which can automatically screen passwords as they are created to ensure compliance.

9. New Web Requirements. The base communications unit must approve all new requirements for AFSPC Web servers, browsing software and authoring tools. In many instances, a single Web server can serve the needs of several or all base organizations. Validate requirements through the standard Communications Systems Requirements Documentation process defined at the HQ AFSPC, NAF and wing levels.

10. Forms Prescribed. Any organization in AFSPC wishing to create or modify a World Wide Web Page will use an AFSPC Form 12, World Wide Web Page Request. This form is available electronically and through your local Publications Distribution Office.

JOHN L. WOODWARD JR., Maj Gen, USAF
Director, Communications and Information

Attachment 1

GLOSSARY OF REFERENCES AND TERMS

References

Paperwork Reduction Act of 1995.

Deputy Secretary of Defense Memorandum, 17 Feb 95, Clearance Procedures for Making Electronic Information Available to the Public.

Secretary of the Air Force Memorandum, 25 May 95, Air Force Policy Guidance on Making Electronic Information Available to the Public.

DoD Directive 5230.9, Clearance of DoD Information for Public Release.

DoD Directive 5500.7-R, Joint Ethics Regulation.

AFI16-201, Disclosure of Military Information to Foreign Governments and International Organizations.

AFI33-129, Transmission of Information Via the Internet.

AFI35-205, Air Force Security and Policy Review Program.

AFI61-204, Disseminating Scientific and Technical Information.

Terms

Base Home Page—Displays information about a specific base. The host wing's Public Affairs unit maintains this page.

Browser—The program running on a computer used to access the Web. This client software browses the Web pages and outputs the information to the computer screen in a readable format.

Combined Military Information—Military Information that, by agreement, is shared by the United States and another government or international organization, regardless of which party to the agreement produces the information.

Controlled Unclassified Information—Unclassified information to which access or distribution limitations have been applied in accordance with national laws, policies, and regulation of the originating country. It includes US information that is determined to be exempt from public disclosure in accordance with DoD Directives 5230.25 and 5300.7 or that is subject to export controls in accordance with the International Traffic in Arms Regulations (ITAR) or the Export Administration Regulations.

Encryption—Encodes data, protecting the information from access during transmission. Software on the intended receiver's side decrypts the data for use.

Export-Controlled Technical Data—Data that can not be lawfully exported without the approval, authorization, or license under US export control laws. The controlling regulations and documents are the ITAR, the US munitions list, and the military critical technologies list.

Firewall—A system of hardware and software which acts as a barrier to incoming and outgoing Internet traffic.

FOUO—For Official Use Only is not a security classification. Information marked FOUO must meet the criteria for Freedom of Information Act Exemptions 2-9 (AFI37-131, para 26.)

Government Limited Access—The Web Servers blocks all traffic except those within the .gov (government) or .mil (military) registered servers from seeing a page. While not secure for use of classified, this does block much of the non-official business traffic. Assume that any government employee or contractor could see this data.

Home Page—The terminology normally associated with a Web HTML document. Normally it is the default first page or “index” of an agency’s information.

HyperText Links (or Link)—As its name implies, a link connects one Web page to another Web page. The link typically appears in highlighted text on a home page. As the cursor touches the link, the cursor takes a different form (usually a hand). Clicking the mouse button causes the Web browser to connect to the page pointed to by the link.

HyperText Markup Language (HTML)—The language one uses to format information for the Web. HTML is a subset of the Standard Generalized Markup Language (SGML), which is the standard for structuring text among desktop publishing applications. HTML allows the user to create multi-media interactive documents with images and forms, for the Web.

International Traffic in Arms Regulation (ITAR)—Controls the export of defense articles specified in the US Munitions List and the technical data directly related to them.

Internet—The conglomeration of hardware and protocols which interconnects Local Area Networks (LANs) in order to form one global network. The Internet is a worldwide conglomeration, and thus, not regulated by state or federal agencies. The Internet Engineering Task Force (IETF), a board of engineers largely from industry, generally addresses Internet issues, but restricts recommendations to hardware and software standards, not policy on Internet usage.

Internet Protocol Address—The address which defines the your Internet connection location. These addresses are grouped into domains including: .mil, .gov, .com, .edu, etc.

Military Critical Technologies List (MCTL)—The list issued by DoD under the authority of the Export Administration Act. The MCTL lists technologies not processed by countries to which the United States controls exports, and which, if exported, would permit a significant advance in a military system of any such country.

Organizational Home Page—Displays information about a specific HQ AFSPC directorate, NAF or wing. The Public Affairs office at either HQ AFSPC, the NAF or the appropriate wing maintains this page. There may be many organizations on a particular base.

Page Owner—The individual responsible for updating and maintaining particular Web pages.

Privacy Act Information—All Privacy Act information is FOUO, for example: name, home address, social security number (see AFI37-132).

Public Release Information—Information approved for public release by appropriate authorities and has no access or protection controls to restrict access to the information. This information requires review by Public Affairs.

Release Authority—This is the person who gives the final approval for the posting of Web pages. This person is ultimately responsible for the validity and security classification of the information placed on the Web.

Restricted Access—Approving officials reserve this access for that information which, while not

classified might be sensitive, or cause unneeded traffic on the page's server. Restricted access should be done for "local personnel only" applications, or those requiring special handling and passwords. Place this information behind a firewall to assure minimal usage and maximum protection.

Technical Data—Classified information relating to defense articles and defense services, or Information covered by an invention secrecy order, or Information which is directly related to the design, engineering, development, production, processing, manufacture, use, operation, overhaul, repair, maintenance, modification, or reconstruction of defense articles.

Unclassified-Sensitive Information—Same as unclassified controlled information. Information which requires protection according to DoD Directive 5200.20, AFI61-204, and the Military Critical Technologies List.

Uniform Resource Locator (URL)—The addressing scheme used in the Web that can reference any type of file on the Internet, enabling a Web user to access that file; contains information about the method of access or protocol, the location of the server and the path name of the viewable files.

Web Document—Similar in information content to any professionally produced document or journal article. The web document is composed of a home page, logical pages, and links. Instead of flipping through pages to read a section of interest, you simply click on a link, displaying a new Web page containing the information of interest. Like articles and documents produced using paper, a Web document contains graphics. But unlike hard copy, a Web document can also contain multimedia information, i.e., video and sound.

Web Server Administrator ("Web Master")—The individual responsible for the World Wide Web server's daily operations, the systems administrator for a Web server. This person or office is responsible for all AFSPC Web pages on a particular base.

World Wide Web (Web)—Software and protocols developed to enable the sharing of information, using client/server technology, through the Internet. Information can be hypermedia; meaning it may be text, graphics, audio, or video files, or any combination thereof.

Attachment 2

FORMAT FOR AN ORGANIZATION HOME PAGE (HQ AFSPC, NAF, WING, GROUP, UNIT - ACCESS THE SAMPLE PAGE THROUGH THE AFSPC/SC HOME PAGE)

A2.1. In the upper left corner, display the organization's shield. *NOTE:* Recommend minimal use of graphics on home pages since they increase the amount of data and time needed to send this information over the Internet. Recommend graphic (.gif) files of less than 20KBs and home pages containing no more than 60kbs of total information. Make graphics to accommodate the lowest screen resolution of 640 X 420 pixels.

A2.2. To the right of the shield, identify the organization by name, e.g., "Headquarters Air Force Space Command (HQ AFSPC)."

A2.3. Below the shield, use the HTML links pointing to:

A2.3.1. Mission Statement and Goals.

A2.3.2. Commander and Key Staff.

A2.3.3. Telephone and E-Mail Directory.

A2.3.4. Units (list all units which report to the organization's commander). Link to both the wings and the bases where they are located.

A2.3.5. Programs, Projects and Bulletin Boards (link to local activities or projects.) This is where you will place applications with limited or local access such as Contracting, CE, Metrics, Bulletin Boards, etc.

A2.3.6. Air Force Space Command Link.

A2.4. Below the above, include the required standard government warning (paragraph 6.4.).

A2.5. For questions on this page contact: (name, office symbol, phone, e-mail address) and date of the last page update.

Attachment 3

FORMAT FOR A BASE HOME PAGE (ACCESS THE SAMPLE PAGE THROUGH THE AFSPC/SC HOME PAGE)

A3.1. At the top of the page include: “Welcome to XX Air Force Base Location.”

A3.2. Include a meaningful photo or graphic of a historic landmark/site on the base. **NOTE:** Recommend minimal use of graphics on home pages since they increase the amount of data and time needed to send this information over the Internet. Recommend graphic (.gif or .jpg) files of less than 20KBs and home pages containing no more than 60kbs of total information. Make graphics to accommodate the lowest screen resolution of 640 X 420 pixels.

A3.3. Following the picture, point (using HTML links) to the following information. **NOTE:** Where applicable, AFSPC organizations should point to AFSPC Link for available command specific information:

- A3.3.1. Base Fact Sheet.
- A3.3.2. Base Personnel Locator.
- A3.3.3. Base Services.
- A3.3.4. Maps of Interest.
- A3.3.5. Host Wing (Link to wing Page).
- A3.3.6. Tenant Units.
- A3.3.7. Programs, Projects and Bulletin Boards.
- A3.3.8. Headquarters, Air Force Space Command Link.

A3.4. Include the required standard government warning notice (paragraph**6.4**).

A3.5. For questions on this page contact: (name, office symbol, phone, e-mail address) and the date of the last page update.