

AR 25-1 Appendix M-11 (USAREUR Web Policy)

M-11. OFFICIAL PUBLIC WEBSITES AND WEBPAGES

a. General. Public websites in the Army in Europe are aligned in the shape of a pyramid, with the USAREUR Homepage on top and subordinate-command homepages below.

b. Oversight of Websites. Commanders and public affairs officers (PAOs) will monitor public websites and their associated webpages. These websites are subject to review by the Office of the G6, HQ USAREUR/7A; and the Office of the Chief, Public Affairs (OCPA), HQ USAREUR/7A, to ensure that they provide current information, continue to provide a useful public service, and present a positive image of the Army in Europe.

c. Responsibilities and Procedures for Establishing Homepages.

(1) Office of the G6. The Office of the G6 is the approval authority for--

(a) Information management and information technology resources used to establish homepages.

(b) Waiver requests to use commercial Internet service providers.

(2) OCPA. The OCPA--

(a) Is the approval authority for and final-decision authority on the contents of public homepages.

(b) Will maintain a registry of public websites.

(c) Will operate and manage computer servers that host public websites in the Army in Europe.

(3) Other HQ USAREUR/7A Staff Offices. HQ USAREUR/7A staff offices may be asked to review proposed or existing webpages for the currency and appropriateness of the information presented (for example, Office of the GE, HQ USAREUR/7A, for information on exercises; Office of the G1, HQ USAREUR/7A, for personnel-related information).

(4) PAOs. PAOs will--

(a) Validate the need for establishing homepages during the information management acquisition request (IMAR) submission process ([para M-12](#)).

(b) Periodically require activities with established websites and webpages to--

1. Justify the continued need for the website or webpage.

2. Verify the currency of information on the website or webpage.

(c) Ensure command homepages are registered with the OCPA.

(5) USAREUR Information Assurance Program Manager (IAPM). The IAPM will--

(a) Coordinate with the Regional Computer Emergency Response Team, Europe (RCERT-E), to ensure that a database of registered Army in Europe webservers is maintained. The 5th Signal Command (5th Sig Cmd) will scan the Army in Europe "electronic footprint" as necessary to identify unregistered servers and may, in coordination with the proponents of this supplement, disable these servers by blocking access until they are registered. The OCPA will notify violators by e-mail or memorandum. Violators will have 5 workdays to register their servers.

(b) Coordinate with the Network Operations and Security Center and the RCERT-E to--

1. Restrict public access to private websites in the Army in Europe through the Internet.

2. Ensure appropriate detection of and reaction to unauthorized or illegal actions against servers hosting public websites in the Army in Europe.

(c) Update policy relating to security aspects of Internet access, coordinate these updates with the Chief Information Officer Council of Colonels, and publish updated policy in this supplement and in the Army in Europe Bulletin.

(6) Commanders and Heads of Organizations. Commanders and heads of organizations with homepages and webpages will--

(a) Ensure security accreditation is accomplished according to AR 380-19 and that webservers are registered with the RCERT-E before they are placed on-line or put in service.

(b) Maintain the currency and accuracy of homepages and webpages by conducting periodic reviews with concurrent staff approval from the supporting PAO for updates to webpage information. Documentation will be maintained to show that required approvals for updates have been obtained. Reviews will also verify that only official or authorized business is being conducted using Government resources and that items posted on the Internet do not discredit or embarrass the Army in Europe.

(c) Be responsible for the actions of their soldiers and civilian employees relating to the use of the Internet and Government resources used to access the Internet.

d. Website Modification. Organization PAOs may approve updates and modifications to websites. In the absence of a PAO, the commander may approve updates and modifications.

e. Website Restrictions. The following will not be placed on public websites:

(1) Classified information.

(2) Unclassified information concerning intelligence activities, cryptologic activities related to national security, or the command and control of forces.

(3) Records and other information that is exempt from release under the Freedom of Information Act. This material is For Official Use Only (FOUO).

(4) Personal information protected by the Privacy Act.

(5) Material that presents a negative image of the Army and the Army in Europe.

f. Links to Other Websites. Homepages often provide links to other Army, DOD, Government, and educational homepages.

(1) Public websites will not provide links to intranet or other restricted-access sites. Links to advertising, product endorsements, and inappropriate non-Federal entity (NFE) websites are also prohibited.

(2) Commanders may approve links to NFE websites that provide a demonstrable benefit to soldiers, DA civilians, and family members, and contribute to telling the Army story in Europe. Webpages that provide links to NFEs must display the disclaimer notice in [figure M-1](#).

g. Clearing Information for Public Release. Information must be cleared for public release before being placed on the Internet. Public Law 100-235, AR 25-55, AR 340-21, and AR 360-1 provide policy on preparing information for public release and distributing this information through the Internet. FM 46-1 authorizes only the commander and the PAO to release information on behalf of the command.

(1) Homepage and webpage content will be strictly controlled to ensure that the information provided is approved for release and is current and appropriate.

(a) Each homepage will have a designated webmaster who is responsible for its content. The homepage will include the name of the webmaster's

organization and the webmaster's mailing address, e-mail address, and telephone number.

NOTE: Organizations should designate an alternate webmaster to act in the absence of the primary webmaster. The organization commander or director should not be the webmaster.

(b) Documentation will be kept on file for each webpage to record the PAO's approval to release the information on the page. This documentation will include the date that the information on the page should be removed or reviewed.

(2) Only actions and documents that are completed, properly cleared, and released will be placed on public websites. "Under construction" pages will not be used.

(3) Information intended only for the official business of internal audiences will not be placed on public websites.

h. Requests for Information. Organizations that maintain websites are responsible for responding to requests for information from the public generated by the website. Organizations that provide information must comply with the Freedom of Information Act.

i. Isolating Public Websites.

(1) To isolate public websites from the rest of the Army Nonsecure Internet Protocol Router Network (ANIPRNET) and reduce the threat of hackers, public websites will be moved to servers maintained and operated by the OCPA. The website's owning organization will continue to maintain the contents of the website. The plan for moving websites to these servers will be published later. Until the movement to OCPA servers is complete, servers hosting unit and activity webpages will be used only to host the webpage and will be isolated from local area networks (LANs).

(2) The USAREUR IAPM iAssure at <https://iassure.usareur.army.mil> provides guidance on isolating websites.

j. Privacy and Data Collection. Because Army systems and networks are subject to monitoring, units and activities with public websites must advise users that use of these systems and networks may be monitored.

(1) Privacy and Security Notice. Organizations that maintain public websites must display a privacy and security notice similar to the one shown in [figure M-2](#). The notice must be displayed in a prominent location on at least the first page of all major sections of the website. A link to this notice should be included on all other webpages. This notice--

(a) Should be tailored to the sponsoring organization and approved by the appropriate local legal authority before being added to the website.

(b) Must clearly inform visitors of the purpose of the website.

(2) Data Collection. For management purposes, statistical summary information and other, nonuser-identifying information may be gathered for assessing website use, determining design specifications, and monitoring system performance and problem areas.

(a) If information is collected, the privacy and security notice will state what information the activity collects about individuals, why it is being collected, and how it will be used. An example of the specific information being collected should be provided. The appropriate legal authority should review documentation on proposed data collection before the collection is initiated to ensure its validity.

(b) The use of "persistent cookies" (those that can be used to track users over time and across different websites) is prohibited unless expressly authorized by the Secretary of Defense.

k. Websites Directed at Children. Special consideration is required for websites directed at children. These websites must comply with the Children's Online Privacy Protection Act of 1998 if personal information is collected.

DISCLAIMER

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

Figure M-1. Disclaimer Notice

PRIVACY AND SECURITY NOTICE

1. This site is provided as a public service by (organization name).
2. Information on this site is considered public information and may be distributed or copied for noncommercial

purposes. Use of appropriate byline, photograph, and image credits is requested.

3. For site management, information is collected for statistical purposes. This Government computer system uses software programs to create summary statistics that are used for purposes such as assessing what information is of most and least interest, determining technical-design specifications, and monitoring system performance and problem areas.

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

5. Except for authorized law-enforcement investigations, no other attempts are made to identify individual users or their use habits. Raw-data logs are used for no other purposes and are scheduled for regular destruction in accordance with National Archives and Records Administration General Schedule 20.

6. Unauthorized attempts to upload or change information on this system are strictly prohibited and may be punishable under the Computer Fraud and Abuse Act of 1987 and the National Information Infrastructure Protection Act.

Figure M-2. Sample Privacy and Security Notice

M-12. ESTABLISHING HOMEPAGES

Commands and organizations that want to establish official public homepages in the Army in Europe will complete and submit an IMAR according to [appendix K](#). Unit PAOs will validate the need for the homepage before the IMAR is submitted. Homepage approval will be provided jointly by the Office of the G6 (for technical approval) and the OCPA (for content approval).

NOTE: An IMAR is required only for homepage approval; it is not needed for updating websites.

a. IMARs.

(1) In addition to the information specified in [appendix K](#), documentation requesting establishment of a homepage must address the following:

(a) The purpose of and justification for the homepage, including site-unique services, information to be provided, and keywords for indexes (for example, Power Projection, Visions, Force XXI Strategy).

(b) Designation of the webmaster responsible for homepage content and appearance.

(c) Required frequency of updates.

(d) A description of planned links to other servers.

(e) A proposed table of contents.

(f) A drawing of the proposed homepage with logos, headers, statements, and uniform resource locators defined.

(2) **Figure M-3** shows the format for IMARs used to request the establishment of a homepage.

b. IMAR Submission.

(1) Requesters will send the IMAR by e-mail through command channels to the appropriate Army in Europe command-approval authority. The approval authority will approve or disapprove the requirement for the website. If the IMAR is approved, the approval authority will annotate it and send it to the G6 (AEAIM-A-S).

(2) The Office of the G6 will coordinate the IMAR with 5th Sig Cmd for network and other technical considerations. If Office of the G6 approves the IMAR, it will send it to the OCPA for final requirements, content approval, and homepage registration.

(3) After it approves, the OCPA will return the IMAR to the requester for implementation.

Subject line of e-mail message: ISPPS-IMAR-(unit identification code (UIC)) (for example, ISPPS-IMAR-WATLAA)

1. ORIGINATOR INFORMATION.

- a. Unit or organization.
- b. POC.
- c. Telephone number.
- d. E-mail address.

2. ITEMS TO BE REPLACED. (Leave blank.)

3. COMPONENT ACQUISITION INFORMATION.

- a. SECURITY CLASSIFICATION CODE: (Enter the appropriate code.)
- b. FUNCTION/PROCESS CODE: (Enter the appropriate code from the Office of the G6 Homepage (<https://www.dcsim.hqusareur.army.mil/plans/ispps/ispps.asp>.)
- c. INFORMATION MANAGEMENT EQUIPMENT (IME) DISCIPLINE/CONFIGURATION CODE: (Enter

"C-HOME PG".)

d. IME CONTRACT: (Leave blank.)

e. CONTRACT LINE ITEM NUMBER: (Leave blank.)

f. DESCRIPTION: (Enter "Establish a (organization name) homepage on the Internet." The organization designation should match the UIC in block 1.)

g. UNIT PRICE: (Enter "\$0". (If contractor development of the homepage is planned, enter the estimated contract amount.))

h. QUANTITY: (Enter "1".)

4. JUSTIFICATION. (Provide specific reasons why the homepage is needed. Include the purpose of and justification for the homepage, site-unique services, information to be provided, and keywords for indexes. The narrative should not exceed one page.)

5. ADDITIONAL INFORMATION.

a. Organization name.

b. Base. (For example, Campbell Barracks)

c. Location. (For example, Heidelberg, Germany)

d. Army in Europe command. (Enter the name of the USAREUR or tenant command ([AE Reg 10-5, app A](#)) or area support group to which the unit or organization belongs.)

e. Commander or equivalent.

f. Homepage name.

g. Tentative homepage address.

h. Webmaster data:

Name

E-mail address

DSN telephone

DSN fax

Civilian telephone

Civilian fax

i. Update frequency.

j. Links. (Provide a list of planned links.)

k. Table of contents. (Provide a list of items that will appear on the homepage.)

l. Proposed homepage layout. (Attach layout.)

Figure M-3. IMAR Format for Requesting Establishment of a Homepage

M-13. ARMY IN EUROPE COMMAND HOMEPAGE AND WEBSITE REQUIREMENTS

a. General. This paragraph establishes minimum requirements for public Army in Europe command homepages and websites and provides a suggested homepage format. Army in Europe commands will ensure that their public homepages and websites meet these standards.

(1) The command website should be used to inform the general public about the command's missions and activities. The website should also provide information about local services available for soldiers, civilians, and their families.

(2) When designing the homepage, commands should keep it simple so that other personnel will be able to maintain the page when the person who created it leaves the command.

b. Required Items. Each Army in Europe command should have only one official homepage that serves as a virtual "visitor center" for the command. The following items are required on Army in Europe command homepages:

(1) **Command Title.** Name of the organization or unit.

(2) **Commercial Link Disclaimer Notice.** The disclaimer notice shown in [figure M-1](#). Army in Europe homepages that have links to NFE websites will include or provide a link to this statement.

(3) **Date of Last Update.** The date when the website was last updated.

(4) **Headquarters Links.** Links to the U.S. Army Homepage (at <http://www.army.mil>) and the USAREUR Homepage (at <http://www.hqusareur.army.mil>). Each organization will also maintain links to its next-higher and next-lower headquarters.

(5) **Housing and Community Information.** A link to the Standard Installation Topic Exchange Service (SITES) system at <http://www.dmdc.osd.mil/sites/owa/showpage?p=index>. The SITES system provides summarized information on key aspects of the moving process and supplements relocation services provided by relocation-assistance offices on major military installations. This site is updated quarterly based on data received from the various installation relocation-assistance offices. This is one of the most important uniform resource locators (URLs) for a website.

(6) **Mission.** A link from the homepage to the organization or unit mission statement. The unit mission-essential task list (METL) may also be included.

(7) **OCPA Seal.** The official seal of the OCPA. Displaying the OCPA seal shows that the OCPA has approved the homepage. The date of approval must be

displayed with the seal.

(8) Privacy and Security Notice. The notice shown in [figure M-4](#). Homepages will include this notice or provide a link to it. Webpages of major sections of websites will provide a link to this notice with the statement "Please read this Privacy and Security Notice."

(9) Subordinate Commands. If subordinate units maintain webpages, the homepage will list these units and their URLs.

c. Recommended Items. The following items are highly recommended to be included in Army in Europe command homepages:

(1) Command Logo. A Joint Photographic Experts Group (JPEG), Graphic Interchange Format (GIF), or other graphic as appropriate that identifies the organization. Each organization should have an appropriate patch or logo that identifies the unit.

(2) Commander's Biography. A link to a black-and-white or color photograph of the commander with the approved biography. The public affairs office is responsible for providing the approved biography and photograph. The command sergeant major's photograph and biography may also be included. Biographies should be limited to the individual's military and professional record. Personal family information, such as children's ages and where they go to school, will not be included.

(3) Cost of Living Allowance (COLA) and Variable Housing Allowance (VHA). A link to information on pay, allowances, COLA, VHA, and other entitlements. This information is available from the Defense Finance and Accounting Service URL (<http://www.dfas.mil>). The URL <http://www.dfas.mil/money/index.htm> may also be used to provide information about financial matters.

(4) Headquarters Organization. A description of the various components of the headquarters organizations and responsibilities.

NOTE: Websites will not display rosters that list names of assigned personnel, personal telephone numbers, individual e-mail addresses, or other personal information such as social security numbers, family-member names, or home addresses. Websites may, however, display lists of duty positions, duty-telephone numbers, and generic duty e-mail addresses (those constructed by using an abbreviated form of the position title, rather than the name of the person).

(5) History. A link to the unit history.

(6) Motto. Unit motto, if the unit has one.

(7) News. A link to a section where news releases may be viewed or downloaded along with feature stories and photographs. Items must be approved by the public affairs office before being placed on the website. Articles must be timely and not left on the page long after the event has taken place.

(8) Other Government Links. Links to other Government websites that would be informative and useful to users. A good start is the URL <http://firstgov.gov/index.shtml> (FirstGov), which is an easy-to-search, free-access website that helps users find information from other U.S. Government agency websites.

(9) Pictures. A link to photographs that enhance the website, particularly photographs that show the unit performing its mission or training for the mission. The public affairs office must approve all photographs before they are placed on the website.

(10) Subordinate Commands. A list of subordinate units and a description of the mission and history of each.

(11) Vision. The organization vision statement. The vision statement informs viewers what the organization expects to achieve in the future.

(12) Weather Information. A link to current weather information. In certain areas, access to weather information is very important. This is recommended only if a noncommercial link can be found.

(13) Welcome Message. A link to a written greeting. This may be accompanied by a short audio recording.

d. Photographic and Graphic Images.

(1) Format. Photographic images must be in JPEG format; graphic images must be in GIF format. JPEG images must be small enough to load quickly using a 28.8 kilobyte (kb) modem. (A 100 kb image needs about 40 seconds to load.) GIF and JPEG image size will depend on the photograph's intended use. Animated GIF files should be used sparingly.

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

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

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

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

(3) Restrictions. Before placing a photograph on the Internet, the webmaster will ensure that posting the photograph will not violate security regulations or embarrass the Army, the unit, or individuals in the photograph. The webmaster may need to consult the commander or PAO to determine whether or not to use certain photographs. Webmasters and photographers will enforce the restrictions of AR 360-1, chapter 5.

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

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

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

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

2. Performing personal hygiene in underwear, which violates propriety.

3. Smoking a cigarette inside a Government building or in a vehicle, which violates Government policy.

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

f. Sample Homepage. [Figure M-5](#) is an example of how a homepage may be arranged.

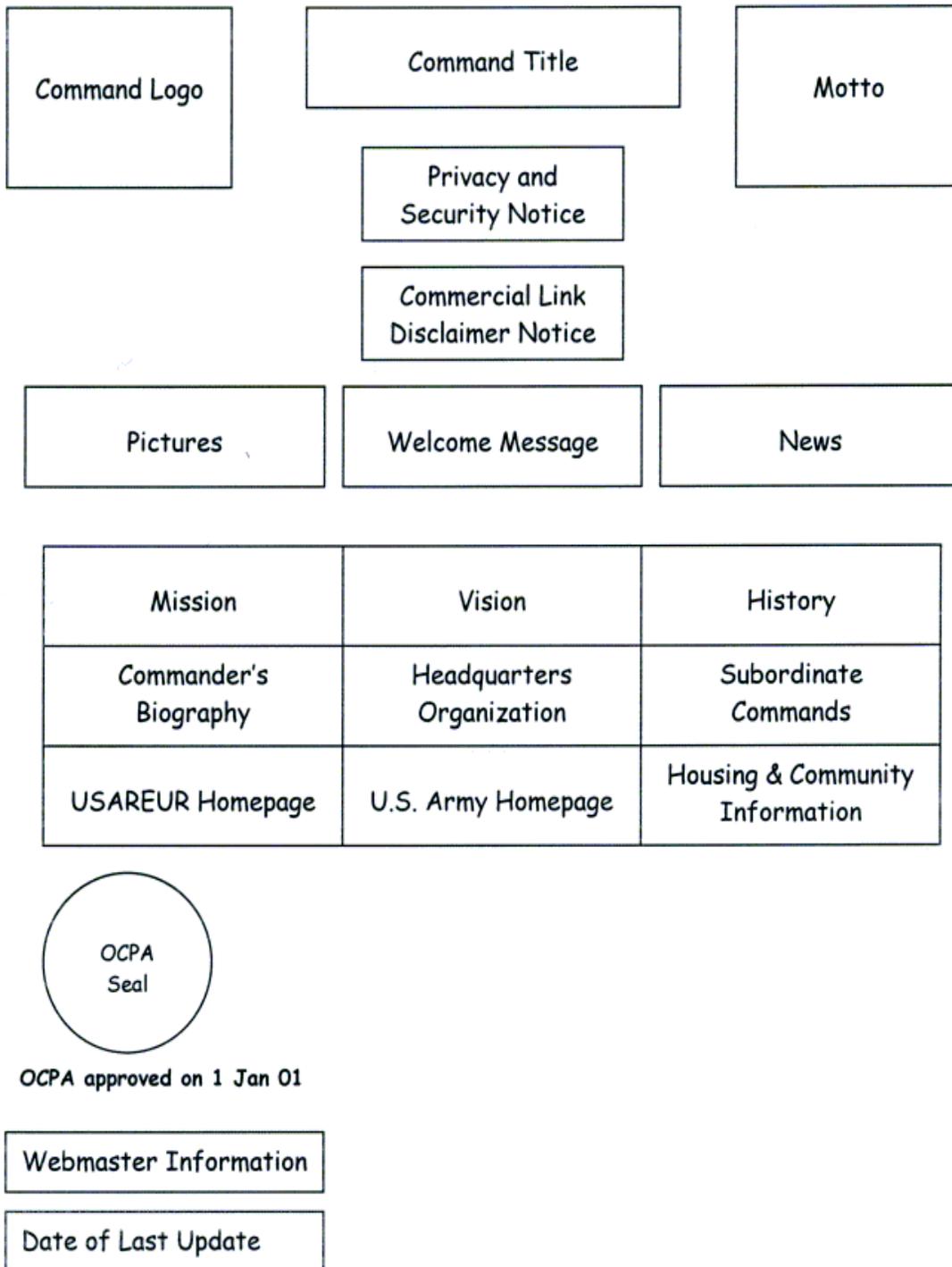


Figure M-5. Sample Homepage

Figure M-4. Sample Privacy and Security Notice

PRIVACY AND SECURITY NOTICE

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

M-14. PRIVATE WEBSITES

a. General. Commands and organizations may establish private websites (intranets) to provide information for use within the Army in Europe, the owning unit, or other target audiences. Unclassified content of private websites is subject to review by the supporting PAO for command-information quality.

b. Security of Private Websites. Administrators of private websites will ensure that appropriate, local-security controls are in place and that the information on the website is accurate, timely, and of use to the organization.

(1) Links. Links will not be made between public and private websites unless controls, such as firewalls, are in place to prevent public access. Units that want to link their private website to a public website must have a valid requirement for the link and no alternative to obtaining the information on the public website.

(2) Servers. Private websites may be on servers owned and maintained by the command. These servers will be--

(a) Protected by security measures applied on the webserver and at the perimeter of the ANIPRNET.

(b) Registered with the RCERT-E to help with the distribution of information assurance vulnerability alerts and to ensure timely responses to security incidents and intrusions.

(3) Protected Access. Private websites may contain unclassified but sensitive information and must be protected from unauthorized or unintended access.

(a) Private websites are required to have a secure sockets layer (SSL) protocol using a class 3 public key infrastructure (PKI) certificate.

(b) Access to private websites may be further restricted through user passwords, server access-control lists, and the use of firewalls between Army LANs and the ANIPRNET.

(4) DOD PKI Initiative. The 5th Sig Cmd webpage at <https://www.pki.5sigcmd.army.mil> provides guidance on obtaining PKI certificates for private webservers. Organization information assurance personnel should also consult with system administrators and public affairs personnel for information on how to protect private websites.