



**MILITARY DEPARTMENT OF ARKANSAS
OFFICE OF THE ADJUTANT GENERAL
CAMP JOSEPH T. ROBINSON
NORTH LITTLE ROCK, ARKANSAS 72199-9600**

MIKE BEEBE
GOVERNOR

WILLIAM D. WOFFORD
MAJOR GENERAL
THE ADJUTANT GENERAL

NGAR-IMS

8 February 2010

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: The Adjutant General's Policy Memorandum 2010-02, Electronic Mail Policy and Procedures

1. REFERENCES.

- a. 5 U.S.C. § 552a, The Privacy Act of 1974.
- b. Health Insurance Portability and Accountability Act (HIPAA).
- c. Act 1287 of 2001, Arkansas annotated code 25-4-110(c).
- d. Paragraph 2-301, DOD 5500.7-R, Joint Ethics Regulation (JER), August 30, 1993, Change 6, 23 March 2006.
- e. AFI 33-119, Air Force Messaging, 24 January 2005.
- f. CPM 380-24, CAC/PKI Guidance for the use of Digital Signature and Encryption.
- g. AR 25-1, Army Knowledge Management and Information Technology, 4 December 2008.
- h. AR 25-2, Information Assurance, 24 October 2007.
- i. AR 25-50, Preparing and Managing Correspondence, 3 June 2002.
- j. AR 25-55, The Department of the Army Freedom of Information Act, 1 November 1997.

NGAR-IMS

SUBJECT: The Adjutant General's Policy Memorandum 2010-02, Electronic Mail Policy and Procedures

k. ALARACT 114/2003 Army Public Key Infrastructure (PKI) Usage Guidance For Encryption and Digital Signing of E-mail Messages.

l. Memorandum, CIO/G-6, Subject: Army Digital Signature Policy memorandum, 29 July 2008.

2. **APPLICABILITY.** This policy complies with DOD, Army and NGB policies and regulations for federal government electronic communications or e-mail and applies to all personnel and organizations of the Arkansas Army and Air National Guard, State Military Department and activities. Commanders and supervisors at all levels will ensure that anyone under their supervision understands and complies with this policy. This policy supersedes TAG policy #99-06 and is effective upon receipt until rescinded or superseded.

3. **OBJECTIVES.** E-mail constitutes official business communications and will be constructed in a clear, concise manner. (AR 25-1)

a. To establish the procedures for e-mail usage in the Arkansas National Guard (ARNG).

b. To maximize the effectiveness and efficiency of e-mail delivery for e-mail users of the ARNG wide-area-network (WAN).

c. To communicate that these procedures exist to ensure adequate storage space, recoverability and records management of e-mail.

d. To communicate that these procedures exist to ensure the stability and reliability of ARNG WAN services.

4. **E-MAIL USAGE.** ARNG federal and state communications systems, to include electronic mail (e-mail), are for official use and authorized purposes only in accordance with (IAW) the JER, DOD and Army regulations and Arkansas Code.

a. Only Government provided e-mail services are permitted. Commercial e-mail services are prohibited unless approved by the DCSIM. Automatically forwarding e-mail from an official government provided account to an un-official commercial, private or personal account is prohibited IAW AR 25-2.

b. All ARNG WAN NIPRNet e-mail communications requiring data integrity, message authenticity, or non-repudiation or containing information that is sensitive,

NGAR-IMS

SUBJECT: The Adjutant General's Policy Memorandum 2010-02, Electronic Mail Policy and Procedures

for official use only (FOUO) or subject to the Privacy or Health Portability Acts will be encrypted and digitally signed. Protections of the Privacy Act include:

(1) Information identified as FOUO. FOUO information is not releasable to the public.

(2) Information protected under HIPPA.

(3) Otherwise sensitive (information and materials requiring present and future restrictive handling) (AR 25-1).

c. All SIPRNet e-mail communications will be no higher than the SECRET classification level and will not be transferred by any means from SIPRNet to a lesser classified network or system except with approved software. ARNG WAN or NIPRNet will not be used to transmit or receive any level of classified information.

d. E-mail communications are federal records and subject to the Freedom of Information Act and the Army Records Information Management System (ARIMS).

e. NIPRNet mailboxes that have not been utilized nor have a log-in every 45 days will be disabled. If they remain inactive for 75 days, the account will be deleted from the network. SIPRNet mailboxes must be logged-in once every 90 days and renewed once per year. If they are not renewed, the account will be terminated. All requests for exceptions to policy for deployment or extended periods of temporary duty will be sent through the IMO to DCSIM for consideration.

5. USER RESPONSIBILITIES. Users are any person, organization, or unit that uses the services of an information processing system. Specifically, it is any command, unit, element, agency, crew or person (Soldier or civilian) operating, maintaining, and/or otherwise using the ARNG WAN products in accomplishment of a designated mission. ARNG WAN NIPRNet or SIPRNet e-mail services or communications will not be used for:

a. Purposes that would reflect unfavorably on the Arkansas National Guard, are incompatible with public service/trust, including, but not limited to text or graphics containing or implying: copyright infringement, intellectual property violations, gambling, spam, chain letters, bulk-mail, off-color jokes, ethnic slurs or victimization based on race, color, religion, gender, national origin, age, or handicap, pornographic/sexually oriented explicit materials or graphics, threatening, harassing, abusive, degrading, deceptive, libelous, defamatory or fraudulent communications.

NGAR-IMS

SUBJECT: The Adjutant General's Policy Memorandum 2010-02, Electronic Mail Policy and Procedures

b. To advertise, solicit business, or engage in other activities in support of a private/commercial business enterprise for personal financial gain or in support of a non-profit organization.

c. For fund-raising activities (except those permitted by the Joint Ethics Regulation).

d. To offer personal items for sale or rent. (The unofficial portion of the Arkansas National Guard PAO update is the authorized electronic bulletin board for posting personal items for sale or rent). Announcements of personal events not connected to government service may be sent to the Daily Guard for publication (dailyguard@ar.ngb.army.mil).

e. For political activities, such as lobbying, soliciting of votes, to include political oriented communications that advocate the support or election of a particular political candidate or party.

f. The use of quotes, slogans, digital graphics/images or backgrounds in e-mail signature blocks, footers or text is prohibited.

g. For unlawful activities that violate public law or Army or DOD policy that would constitute a criminal offense or civil liability.

h. Users will neither knowingly nor willfully transmit viruses, worms or other malicious logic or computer code through text, graphics, attachments or hyper-links.

6. DIGITAL SIGNATURES AND ENCRYPTION. The digital signature provides assurances that the integrity of the message has remained intact in transit, and provides for the non-repudiation of the message that the sender cannot later deny having originated the e-mail (ALARACT 114-2003). This applies to emails originating on workstations physically connected to the network, virtually connected wireless devices (e.g., two-way email devices (TWEDs), Personal Digital Assistants (PDAs), etc.), and remote workstations (i.e., connected using a Virtual Private Network (VPN) or remote access/application publishing programs such as Citrix). Digital Signatures and encryption will be used:

a. When e-mail is considered official business (FOUO) and/or contains sensitive information. (Privacy Act or Health Insurance Portability and Accountability Act, refer to paragraph 4, b, (1)).

NGAR-IMS

SUBJECT: The Adjutant General's Policy Memorandum 2010-02, Electronic Mail Policy and Procedures

b. When e-mail contains embedded hyper-links (URLs) or attachments. Pure text references to web addresses, URLs, or e-mail addresses do not require digital signature; only those with active (clickable) content.

c. Senders will not use digital signatures for personal or routine administrative email messages.

d. Senders will not digitally sign emails sent to non .mil addresses unless a trust relationship has been established through a DOD approved method.

e. All ARNG WAN users will publish their PKI certificates to the Global Address List (GAL) in order to send and receive encrypted e-mail communications. Self-help instructions for publishing the security certificates are available at the following link [Publish certificates to the GAL](#). Select "update outlook security settings (publish certificates to GAL)."

f. Encrypted emails will be digitally signed. While encryption ensures the confidentiality of data, it does not provide data integrity or non-repudiation of the email.

g. When an encrypted e-mail is received, recipients must take appropriate measures to protect the encrypted information. If a message has been encrypted, the implication is that it contains sensitive information that needed to be protected during transmission. Once it has been received, the need to protect the information remains with the recipient. E-mails that are received in encrypted form and contain sensitive information need to be stored in encrypted form to ensure appropriate protection of the information.

h. Signature Blocks. As stated in paragraph 5, f; the use of quotes or slogans are prohibited in e-mail. Signature blocks will be formatted IAW AR 25-50 or as indicated below:

JOHN P. DOE

COL, QM

DOL, G-4

(501) 212-XXXX

FAX: (501) 212-XXXX

(optional inclusion of e-mail address....)

JOHN P. DOE

Chief, Plans Branch

(501) 212-XXXX

FAX: (501) 212-XXXX

JOHN P. DOE

Systems Analyst

Contractor (SAIC, Inc)

(501) 212-XXXX

(1) Contractors will identify themselves in government e-mail correspondence including the name of their company, as shown in the example above.

NGAR-IMS

SUBJECT: The Adjutant General's Policy Memorandum 2010-02, Electronic Mail Policy and Procedures

(2) Confidentiality and Disclaimer Statements. The exception to policy is the use of confidentiality statements and disclaimer statements used by legal, medical, recruiting or inspector general personnel. These statements may be included as part of the signature block. For example:

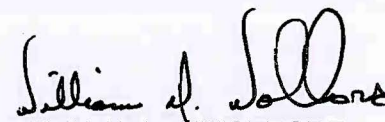
"INSPECTOR GENERAL SENSITIVE INFORMATION-FOR OFFICIAL USE ONLY: The information contained in this e-mail, facsimile, and any accompanying attachments may contain Inspector General sensitive information and is predecisional, which is protected from mandatory disclosure under the Freedom of Information Act, Title 5, United States Code, Section 552. It will not be released to unauthorized persons. If you are not the intended recipient of this information, any disclosure, copying, distribution, or the taking of any action in reliance on this information is prohibited. "

(3) Signature blocks may be formatted automatically using Microsoft Outlook Tools. Open Microsoft Outlook; select "Tools" from the menu, followed by "Options," followed by "Mail Format." Select "Signatures" followed by "New," and follow the instructions. Enter your signature IAW the formatted guidance in this policy and AR 25-50.

7. Violations of this policy may be subject to disciplinary action and penalty IAW Technician Personnel Regulation 752, NGR 600-5/ANGI 36-101, Military Department of Arkansas State Employee Discipline and Adverse Procedures, Arkansas Military Code, or the Uniform Code of Military Justice, as applicable.

8. Service members, federal, state employees and contractors will use federal government communications systems with the understanding that use serves as consent to monitoring, including incidental and personal uses, whether authorized or unauthorized.

9. Questions concerning the appropriateness of using government e-mail for a specific purpose should be addressed to the Staff Judge Advocate (501) 212-5030.



WILLIAM D. WOFFORD
Major General
The Adjutant General

DISTRIBUTION:

A