



DEPARTMENT OF THE NAVY

CHIEF OF NAVAL AIR TRAINING
CNATRA
250 LEXINGTON BLVD SUITE 102
CORPUS CHRISTI TX 78419-5041

CNATRAINST 5230.7

N6

'28 OCT 2008

CNATRA INSTRUCTION 5230.7

Subj: CNATRA ELECTRONIC MAIL (E-MAIL) DIGITAL SIGNATURE AND
ENCRYPTION POLICY

Ref: (a) DODI 8520.2
(b) DON CIO Washington DC/02041ZAUG2007
(c) JTF-GNO CTO 07-015 Revision 1
(d) NAVADMIN 248/08
(e) CNO Washington DC/071651ZDEC2004
(f) DODD 8500.1
(g) PKI Roadmap for the DOD 04SEP01
(h) CNATRAINST 5000.2C

1. Purpose

a. Provide policy in support of the Public Key Infrastructure (PKI) as defined in reference (a), which enhances the security of Department of the Navy (DON) information systems within Chief of Naval Air Training (CNATRA) and Naval Air Training Command (NATRACOM) by utilizing digital signatures and encryption.

b. Define procedures and guidelines for the effective implementation of CNATRA E-mail Digital Signature and Encryption Policy.

2. Applicability and Scope. This instruction applies to:

a. All CNATRA and NATRACOM personnel to include military, government civilians and contractors using DON information systems.

b. All unclassified E-mails sent from a DON system or account to include, but not limited to, desktops, laptops and Personal Electronic Devices (PEDs) such as Blackberries, as prescribed in reference (b) and (d).

28 OCT 2008

3. Definitions. Terms and definitions used in this instruction are defined in references (d), (f) and (g).

a. Digital Signature. A "stamp" on an email, which is unique to the user and provides an accurate means of identifying the originator of a message (message authenticity). Assures the recipient that the original content of the message or document is unchanged (data integrity). Provides the sender proof of delivery and the recipient with proof of the sender's identity (non-repudiation).

b. Encryption. The process of transforming data to an unintelligible form in such a way that the original data either cannot be obtained (one-way encryption) or cannot be obtained without using the inverse decryption process.

c. Non-Repudiation. Assurance that the sender of the data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so that neither party can later deny having processed the data.

4. Policy

a. This instruction implements the policies and supplements the guidance established in references (a) through (f).

b. Per Department of Defense (DOD) wide requirements, all unclassified official E-mails, sent from a DON system or account that requires message integrity and/or non-repudiation must be digitally signed. This includes E-mails that contain the following:

- (1) Directions, tasks or passes direction or tasking.
- (2) Requests or responses to requests for resources.
- (3) Publishes organization, position or information external to the organization (command, division or department).
- (4) Discusses any operational matter.
- (5) Discusses contract information, financial or funding matters.

28 OCT 2008

(6) Discusses personnel management matters.

(7) The need to ensure that the E-mail originator is the actual originator.

(8) The need to ensure that the E-mail content has not been tampered with during transit.

(9) Active embedded hyperlink.

(10) Attachments.

c. The following do not need to be digitally signed:

(1) Personal or non-official E-mail.

(2) Pure text references to web addresses, Uniform Resource Locators (URLs) or E-mail addresses.

d. In addition to section 4b, official E-mail that contains the following information must also be encrypted:

(1) Sensitive information, as defined in reference (f), such as the following:

(a) Privacy Act

(b) Health Insurance Portability and Accountability Act (HIPAA) Act

(c) Contract information

(d) For Official Use Only (FOUO)

(2) Discusses any information that may be considered as an OPSEC indicator.

5. Responsibility. The CNATRA Command Information Officer (CIO) will ensure compliance with DOD and DON policies and procedures for information systems. Commanding Officers, Special Assistants and Managing Department Heads of CNATRA and NATRACOM will adhere and ensure subordinate adherence to this policy, as specified in reference (h).

12 OCT 2008

6. Contact Information for CNATRA CIO: CNATRA (N6),
250 Lexington Boulevard, Suite 102, Corpus Christi, TX 78419-
5041, DSN 861-1430 or Commercial (361) 961-1430.



JAMES A. CRABBE
Chief of Staff

Distribution:
CNATRAINST 5215.1R
List I & III
CNATRA N6 IAM

Copy to:
NETC