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

CNATRAINST 5230.7A
N6
3 Mar 16

CNATRA INSTRUCTION 5230.7A

Subj: CNATRA ELECTRONIC MAIL DIGITAL SIGNATURE AND ENCRYPTION POLICY

Ref: (a) DODI 8520.02
(b) DON CIO Washington DC/032009ZOCT2008
(c) NETWARCOM CTO 08-07, PKI Implementation
(d) JTF-GNO CTO 07-015, PKI Implementation, Phase 2
(e) NAVADMIN 248/08
(f) CNO Washington DC/071651ZDEC2004
(g) DODI 8500.01, DOD Cybersecurity, 14MARCH2014
(h) PKI Roadmap for the DOD v2.0 29SEP06

Encl: (1) List of Web Links to References

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 (IS) within the 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 Electronic Mail (E-mail) Digital Signature and Encryption Policy.

2. Cancellation. CNATRAINST 5230.7

3. 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 iPhones, as described in references (b) and (e).

4. Definitions. Terms and definitions used in this instruction are defined in references (d), (e) and (h).

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 in 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. Format Sensitive Information. Unclassified information regarding Department of Defense (DOD) capabilities, infrastructure, personnel and/or operational procedures when electronically aggregated in significant volume that could adversely affect the national interest, the conduct of federal programs or the privacy of an individual if lost, misused, accessed, or modified in an unauthorized way. This includes information that may be subject to public disclosure but requires protection when in electronic format.

d. Non-Repudiation. Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents.

e. Sensitive Information. Any information that has not been approved for public release by a public affairs review process. Typically, this refers to For Official Use Only (FOUO), Privacy Act, or Department of State Sensitive But Unclassified (DoSSBU), or Personally Identifiable Information (PII).

5. Policy

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

b. Per 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) Directs, tasks or passes direction or tasking.

(2) Requests or responds 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.

(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 5b, official E-mail that contains the following information must also be encrypted:

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

(a) Privacy Act and Personally Identifiable Information (PII).

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

(c) Contract information.

(d) For Official Use Only (FOUO).

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

6. 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.

7. Contact Information for CNATRA CIO: CNATRA (N6),9035 Ocean Drive, Suite 322, Corpus Christi, TX 78419, DSN 861-3213, Commercial (361) 961-3213.

D. M. EDGECOMB
Chief of Staff

Distribution:
CNATRA Website
CNATRA SharePoint

LIST OF WEB LINKS TO REFERENCES

Note: If clicking the link does not work, try copying the link and pasting it into the web browser.

DODI 8520.02 – PKI and PK Enabling; May 24, 2011
www.dtic.mil/whs/directives/corres/pdf/852002p.pdf

DON CIO Washington DC/032009ZOCT2008, DON Policy Updates for PED Security and Application of Email Signature and Encryption, 03 OCT 2008
http://www.doncio.navy.mil/Download.aspx?AttachID=690

NETWARCOM CTO 08-07, PKI Implementation.
https://infosec.navy.mil/PKI/netwarcom_cto_08-07_pki_im.pdf

JTF-GNO CTO 07-015, PKI Implementation, Phase 2
https://www.cybercom.mil/J3/orders/CTOs/CTO_PKI_Phase2v17%20(11Dec07).rtf

NAVADMIN 248/08 – Implementation of Navy E-Mail Digital Signature Policy – CNO Washington DC 042120ZSEP08
https://infosec.navy.mil/PKI/navadmin_248-08.pdf

CNO Washington DC/071651ZDEC2004, Navy Common Access Card (CAC) and PKI Implementation Guidance Update
https://infosec.navy.mil/PKI/R071651ZDEC04CNOWASHINGTONDCUNCLAS.pdf

DODI 8500.01, DOD Cybersecurity, 14MARCH2014
http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf

PKI Roadmap for the DOD v2.0 29SEP06
https://infosec.navy.mil/PKI/pki_roadmap.pdf