



DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON, D.C. 20350-1000

SECNAVINST 5239.21
DON CIO
27 August 2010

SECNAV INSTRUCTION 5239.21

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY ELECTRONIC SIGNATURE POLICY

Ref: (a) CNSSI 4009, National Information Assurance Glossary, 26 Apr 2010
(b) DoD 7750.07-M, DoD Forms Management Program Procedures Manual, 14 May 2008
(c) Public Law 106-229, Electronic Signatures in Global and National Commerce Act, 30 Jun 2000
(d) Public Law 105-277, Government Paperwork Elimination Act, 21 Oct 1998
(e) Public Law 104-13, Paperwork Reduction Act, 22 May 1995
(f) FIPS 186-3, Digital Signature Standard, Jun 2009
(g) through (m), see enclosure (1)

Encl: (1) References (continued)
(2) Reference Location Table

1. Purpose. To establish electronic signature policy for the Department of the Navy (DON) consistent with Federal and Department of Defense (DoD) policies.

2. References, Terms and Definitions. Location of references is indicated in enclosure (2). Definitions used in this instruction are provided in references (a), (b), and (c).

3. Scope

a. This instruction applies to all DON military, civilian, and contractor personnel.

b. This policy does not apply to any documents that are covered as "exemptions" or "exceptions" within reference (c).

c. The policy and requirements of the DoD and the Federal Government take precedence over any conflicting requirements of this instruction. Implementing authorities should identify conflicting policy to the DON Chief Information Officer (CIO) for resolution.

4. Background

a. Reducing Navy's reliance on paper transactions will improve information security and sharing, allow quicker access to documents, and reduce costs and environmental impact. Streamlining processes that required traditional written signatures and replacing them with electronic signatures, when practicable, is essential to the DON complying with legislative and DoD mandates for paperless processing. References (c) through (f) establish electronic signature policy and requirements for the Federal Government.

b. For this instruction, the term "electronic signature" refers to an electronic sound, symbol, or process attached to, or logically associated with, a contract or other record and executed or adopted by a person with the intent to sign a record (reference (c)).

5. Policy

a. Electronic signatures are to be accomplished using a DoD approved process that utilizes Public Key Infrastructure (PKI) certificates issued by DoD or a DoD approved external PKI. Where personnel have not been issued PKI certificates, functional managers and system owners will determine the appropriate electronic signature tool to use following guidance provided in references (c), (d), (g), and (h). In cases where an electronic signature solution is already in place, organizations will comply with these requirements when performing lifecycle upgrades or a technical refresh.

b. All electronic signature solutions must be certified and accredited per reference (i), and tested and approved for conformance by the Joint Interoperability Testing Command per reference (j).

c. This policy is not a mandate to replace hand-written signatures but rather a policy to adopt electronic signatures as the preferred means of conducting business transactions within the DON.

d. Organizations with applications, systems, and business processes that use electronic signatures shall comply with the following:

(1) Conduct a legal review of the adopted application or process to ensure legal sufficiency, reliability, and compliance with existing laws and regulations. Organizations should consult reference (k) for guidance and conduct legal research to determine the current state of the law in the relevant jurisdiction. A DoD-approved digital signature process, with proper recordkeeping, assures data integrity and non-repudiation and should satisfy most legal sufficiency and reliability concerns. But, conducting a legal review is prudent as unique organizational missions and practices may require processes that provide specific levels of signature security.

(2) Ensure the adopted application or process affords the signer the opportunity to review the information to be signed prior to electronically signing a document. This could be accomplished via a warning or message advising an individual that he or she is about to digitally sign a document. This warning must allow the individual to cancel or exit prior to signing the document. This does not apply to e-mail.

(3) Enable an electronically signed document to be converted to a paper copy as needed or required by law or policy. Archive the paper copy per reference (l). In addition, any converted paper document shall indicate that the document and or form was digitally signed. When the digital signature information is requested or required for record and or legal purposes, the paper copy shall minimally contain:

(a) A statement or other indication that the document or form was digitally signed.

(b) Name of the individual who digitally signed the document or form.

(c) Certificate policy identifier associated with the certificate of the individual who digitally signed the document or form.

(d) Date and time document was signed.

(4) Ensure the integrity of electronically signed documents by retaining digital metadata or adequate contextual materials such that each record can be authenticated, attributed to the signer, and verified to be a full and accurate representation of the transaction to which it attests, to reflect the intent of the signer, and to be complete and unaltered. This provides the proper context and assists in establishing intent when a user signs a particular document as per reference (k).

(5) Archive electronically signed documents following references (l) and (m). Additionally, per references (k) and (m), organizations should at a minimum:

(a) Ensure all of the information required to validate a digital signature remains available for the life of the document.

(b) Ensure the integrity of an electronically signed document in such a manner that records can be determined to be authentic and reliable by tracking the chain of custody and any changes that may occur (authorized or unauthorized) (reference (k)).

(c) Embed the electronic signature in the content of the record, or store it separately if it is not practicable to embed it. If an electronic signature technology separates the signature from the rest of the record, it must be associated in some way and captured in a recordkeeping system to preserve the complete content of the record.

(6) Maintain a list of individuals with knowledge and expertise regarding the various electronic signatures used by the organization so that they can be easily located for use in trial preparation and, if necessary, as witnesses at trial.

SECNAVINST 5239.21
27 August 2010

6. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per reference (m).

A handwritten signature in blue ink, appearing to read "R. J. Carey". The signature is stylized and cursive.

R. J. CAREY
Department of the Navy
Chief Information Officer

Distribution:

Electronic only, via Department of the Navy Issuances Web site
<http://doni.daps.dla.mil/>

REFERENCES (continued)

- (g) OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, 16 Dec 2003
- (h) NIST Special Publication 800-63, ver. 1.0.2, Electronic Authentication Guideline, Apr 2006
- (i) DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), of 28 Nov 2007
- (j) DoD CIO Memorandum, DoD-wide Digital Signature Interoperability, 05 May 2006
- (k) U.S. Department of Justice Publication, "Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies," Nov 2000
- (l) National Archive and Records Administration (NARA) Records Management Guidance for PKI Digital Signature Authenticated and Secured Transaction Records, 11 Mar 2005
- (m) SECNAV Manual 5210.1, Department of the Navy Records Management Program, Records Management Manual, 16 Nov 2007

Reference Location Table

Ref	Subject	Location
a	CNSSI 4009, National Information Assurance Glossary, Jun 2006	http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf
b	DoD 7750.07-M, DoD Forms Management Program Procedures Manual, 14 May 2008	http://www.dtic.mil/whs/directives/corres/pdf/775007m.pdf
c	Public Law 106-229, Electronic Signatures in Global and National Commerce Act ("ESIGN"), 30 Jun 2000	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=106_cong_public_laws&docid=f:publ229.106.pdf
d	Public Law 105-277, Government Paperwork Elimination Act (GPEA), 21 Oct 1998	http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=105_cong_public_laws&docid=f:publ277.pdf
e	Public Law 104-13, Paperwork Reduction Act, 22 May 1995	http://reginfo.gov/public/reginfo/pra.pdf
f	FIPS 186-3, Digital Signature Standard, Jun 2009	http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf
g	OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, 16 Dec 2003	http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf
h	NIST Special Publication 800-63, ver. 1.0.2, Electronic Authentication Guideline, April 2006	http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf
i	DoD Instruction 8510.01, Information Assurance Certification and Accreditation Process (DIACAP) of 28 Nov 2007	http://www.dtic.mil/whs/directives/corres/pdf/851001p.pdf
j	DoD CIO Memorandum, DoD-wide Digital Signature Interoperability, 05 May 2006	http://www.doncio.navy.mil/Download.aspx?AttachID=581

Ref	Subject	Location
k	U.S. Department of Justice Publication, "Legal Considerations in Designing and Implementing Electronic Processes: A Guide for Federal Agencies," Nov 2000	http://www.usdoj.gov/criminal/cybercrime/eprocess.pdf
l	National Archive and Records Administration (NARA), Records Management Guidance for PKI Digital Signature Authenticated and Secured Transaction Records, 11 Mar 2005	http://www.archives.gov/records-mgmt/policy/pki.html
m	SECNAV Manual 5210.1, Department of the Navy Records Management Program, Records Management Manual, 16 Nov 2007	http://doni.daps.dla.mil/SECNAV%20Manuals1/5210.1%20CH-1.pdf