U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
STOP 7101
Washington, DC 20593-7101
Staff Symbol: CG-6
Phone: (202) 475-3518
Fax: (202) 475-3929

COMDTINST 5200.5
FEB 3 2011

COMMANDANT INSTRUCTION 5200.5

Subj: ELECTRONIC SIGNATURES AND MANAGEMENT OF ELECTRONICALLY SIGNED RECORDS

Ref: (a) Information Management and Electronic Government (E-GOV), COMDTINST 5200.1
(b) Information and Life Cycle Management Manual, COMDTINST M5212.12 (series)
(c) The Coast Guard Correspondence Manual, COMDTINST M5216.4 (series)
(d) Government Paperwork Elimination Act (GPEA), Pub. L. 105–277, div. C, title XVII, Oct. 21, 1998, 112 Stat. 2681–749; see 44 USC § 3504 note
(e) Appendix II to OMB Circular No. A-130, Implementation of the GPEA (Nov. 28, 2000)
(f) National Archives and Records Administration (NARA) Records Management (RM) Guidance for Agencies Implementing Electronic Signature Technologies (March 11, 2005)
(g) U.S. Coast Guard Information Assurance (IA) for Unclassified Information Systems, COMDTINST 5500.13
(h) Public Key Infrastructure (PKI), COMDTINST 5500.20

1. PURPOSE. The purpose of this Instruction is to establish Coast Guard policy regarding the use of electronic signatures and management of records with an electronic signature.

2. ACTION. All Coast Guard unit commanders, commanding officers, officers-in-charge, deputy/assistant commandants, and chiefs of headquarters staff elements shall comply with the provisions of this Instruction. Internet release is authorized.

3. DIRECTIVES AFFECTED. None.

4. DEFINITIONS. The following definitions apply to this Instruction.

   a. "Digital signature(s)" means the owner of a private signing key uses that key to create a unique mark (the signature) on an electronic document or file. The recipient employs the owner's public

DISTRIBUTION – SDL No. 158

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	1	1	1	1	1	**1**	1	1	1	1		1	1	1	1	1	1		1		1	1				
B	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
C	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
D	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
E	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1		
F																	1	1	1							
G		1	1	1	1																					
H	1	1	1	1	1	1	1																			

NON-STANDARD DISTRIBUTION:

key to validate that the signature was generated with the associated private key. This process also verifies that the document was not altered. A digital signature is a technology that provides a valid method of electronic signature.

b. “Electronic signature(s)” means a method of signing an electronic record that:

(1) identifies and authenticates a particular person as the source of the electronic record; and

(2) indicates such person's approval of the information contained in the electronic record." See reference (d), § 1709(1). This definition is consistent with other accepted legal definitions of signature. The term "signature" has long been understood as including "any symbol executed or adopted by a party with present intention to authenticate a writing." Uniform Commercial Code, 1-201(39)(1970)). The "Uniform Electronic Transactions Act," adopted by the National Conference of Commissioners of Uniform State Laws contains a similar definition. (See http://www.nccusl.org). This flexible definition permits the use of different electronic signature technologies, including but not limited to digital signatures, personal identifying numbers, and biometrics. The electronic signature process involves authentication of the signer’s identity; binding of the signature to the document; and non-alterability after the signature has been affixed thereto.

c. “Records” are defined as including “all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them (44 U.S.C. 3301)." This also includes, but is not limited to, microfilm, audiovisual materials, automatic data processing documents or databases, and electronic mail (e-mail).

d. “Temporary records” are those records that have been appraised by the Archivist of the United States as having a finite retention based on determined administrative, fiscal, and legal value. Generally, these files may be transferred to Federal Records Centers (FRCs) for storage in hard copy. For those records stored at FRCs, agencies are informed prior to final disposition per the instructions of Sections II and III of the Information and Life Cycle Management Manual reference (b), at p. I-1-5. Eligible temporary records are destroyed or deleted per disposition instructions in reference (b). For example, Time Cards are destroyed after GAO audit or when 6 years old, whichever is sooner; and SAR cases not selected as having historical significance are destroyed 10 years after final closing of the case.

e. “Permanent record(s)” means those records that have been appraised as having enduring historical, research, legal, scientific, cultural, or other values. Coast Guard’s permanent records are those that will protect interests and document the primary missions, functions, responsibilities, and significant accomplishments of the agency. Eligible permanent records are sent to NARA for preservation in the National Archives of the United States and made available to the public for historical research, per disposition instructions in reference (b), at p. I-1-4. Examples are:

(1) The official record copy of each directive/publication issued, with significant background material;

(2) SSIC 2000/4e Electronic Engineering Records- Case files on electronic navigational aids containing request for authorization, approvals for installation, photographs, blueprints, correspondence, related papers on changes and maintenance; and

(3) SSIC 16450/13 Records of meetings of the Marine Safety Council.

f. "Information System" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. An Electronic Information System (EIS) is a system that contains and provides access to computerized Federal records and other information (36 CFR 1234.2).

g. "Scheduling" means the process by which an agency obtains NARA approval for the disposition of agency records when agency business need for the records ceases, i.e., destruction of temporary records and transfer to the National Archives of the United States of permanent records. (36 CFR 1228, Subpart B).

5. SCOPE. This Instruction applies only to Coast Guard records that use an electronic signature.

6. DISCUSSION.

a. The Coast Guard has established policy regarding the life cycle management of records, outlined in references (a) through (c). References (d) through (h) provide legal and policy requirements for use of electronic signatures by federal agencies.

b. Coast Guard personnel use a Common Access Card (CAC) to access and use most, but not all, Coast Guard information systems. CACs provide a unique identifier and means of authentication of all Coast Guard electronic records. Further, automated technology on the Standard Work Station provides the means to use electronic signatures for records such as email, memoranda, letters, and certain forms. Reference (d), at section 1707, provides that "[e]lectronic records submitted or maintained in accordance with procedures developed under this title, or electronic signatures or other forms of electronic authentication used in accordance with such procedures, must not be denied legal effect, validity, or enforceability because such records are in electronic form."

c. The Coast Guard secures Public Key Infrastructure credentials embedded in the DOD issued Common Access Card. The electronic certificates on an individual's CAC are the essential elements to the creation of a valid electronic signature.

7. POLICY. Coast Guard policy regarding digital signatures continues to evolve. Currently, the following applies to use of digital signatures on Coast Guard Standard Workstations.

a. Authorization. Units are authorized to sign records with electronic signatures, using individual CAC and the office automation applications embedded within the Coast Guard Standard Workstation Image. Unit commanders, commanding officers, officers-in-charge, deputy and

assistant commandants, and chiefs of headquarters staff elements, may, at their discretion, withhold for any record authority to use electronic signatures.

b. Electronic signatures shall:
   (1) Only be used by the original individual to whom the digital signature is assigned.
   (2) Not be delegated to a subordinate, alternate, or "On Behalf Of" representative.
   (3) Be inspected prior to archiving to ensure the electronic document has been permanently encapsulated to prevent any alteration of the data or metadata associated with the electronic document.
   (4) Be considered invalid if the electronic document has been altered or otherwise not permanently encapsulated by the office automation application.
   (5) Be considered invalid if electronically signed by an expired means of authentication such as CAC, any other electronic signature token, certificate, or Public Key Infrastructure device.
   (6) Only be used in instances in which the receiving or third party will accept a digital signature. In cases where this does not apply, e.g. for certain contracts, hard copy must be used and maintained.

c. The Command, Control, Communications, Computer and Information Technology Service Center (C4IT SC) shall update procedures for standardizing the data format for electronic signatures. While this will include the signer's name, date and other pertinent information residing in a standard electronic signature field, the onus to include the name of the command/directorate resides with the signatory official.

d. As the CG Standard Workstation Image with embedded standard office automation applications are updated, the C4IT SC is responsible for ensuring that the office suite and standard applications have a proper audit trail that supports the integrity of electronic signatures.

e. Legal sufficiency. Records with electronic signatures submitted in accordance with the GPEA are presumed legally sufficient, valid, and enforceable.

f. Management of records having electronic signatures. Unit commanders, commanding officers, officers-in-charge, deputy and assistant commandants, and chiefs of headquarters staff elements shall control the creation, use, maintenance, and disposition of e-mail and electronic documents in accordance with paragraph g. below. Subject records shall be sufficiently labeled to enable authorized personnel to retrieve, protect, and dispose of them per legally prescribed dispositions. Identifying information includes office of origin, promulgating official's name, the Standard Subject Identification Code (SSIC), key words for retrieval, addresses, and security classification, if applicable. Electronic storage will reflect the office File Plan (Form CG-6022), which is the itemized, up-to-date list of records in a designated office/unit, containing a brief description of their content, SSIC numbers(s), location and disposition instruction. Commands shall ensure the maintenance of electronically signed documents is addressed during upgrades/migrations of software, hardware and systems used to create and/or store the records.

   (1) Temporary records. Temporary records may have traditional pen and ink signatures, or employ electronic signatures using any technology available on standard information systems. Records may be maintained electronically, provided they are categorized and maintained in accordance with reference (b) (Section II, SSICs) until they are eligible for disposition

(destruction). Temporary electronic records are not stored in a Federal Records Center and are not transferred to NARA.

(2) Permanent records. Permanent records may have traditional pen and ink signatures, or employ digital signatures using technology available on standard information systems. They must be transferred to NARA per the life cycle for the specific series, as outlined in reference (b). Electronic records must be in a scheduled information system or database in order to complete the transfer to NARA.

g. Storage of records having electronic signatures.

(1) Units are directed to store records with electronic signatures on a Coast Guard electronic file storage system. The file storage system must employ a disaster recovery system and support the backup of records with a frequency that assures complete recovery. Records with electronic signatures should not be stored on standalone or external systems or hardware.

(2) Units must monitor electronic records to ensure that the records maintain data integrity, accessibility and readability until final disposition.

8. DIGITAL SIGNATURE EXECUTION. Guidance regarding use and implementation on the Standard Workstation is available on the Telecommunication and Information Systems Command (TISCOM's) site on the CG Portal.

9. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATIONS. Environmental considerations were examined in the development of this directive and have been determined to be not applicable.

10. FORMS/REPORTS. None.

R. E. Day /s/
Assistant Commandant for Command,
Control, Communications, Computers, and
Information Technology