DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 5239.24
OCIO
22 Jul 2019

SECNAV INSTRUCTION 5239.24

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY DIGITAL SIGNATURE POLICY

Ref: (a) DoD Instruction 8520.02 of 24 May 2011
(b) 15 U.S.C. §7001, et seq.
(c) 44 U.S.C. §3504
(d) OMB Circular A-130, Managing Federal Information as a Strategic Resource of 28 July 2016
(e) Federal Chief Information Officers Council Guidance, Use of Electronic Signatures in Federal Organization Transactions of 25 January 2013

1. Purpose. To maintain and update digital signature policy for the Department of the Navy (DON) consistent with Department of Defense (DoD) policies and other applicable law, regulation and policies.

2. Cancellation. SECNAVINST 5239.21.

3. Applicability

a. This instruction applies to the Offices of the Secretary of the Navy, the Chief of Naval Operations, the Commandant of the Marine Corps, and all U.S. Navy, U.S. Marine Corps installations, commands, activities, field offices, and all other organizational entities within the DON.

b. 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. Policy

a. It is DON policy to adopt digital signatures as the preferred means of conducting business transactions within the DON. This policy does not prohibit physical signatures, but

digital signatures enable authentication of electronic documents and assure both the identity of the sender and the integrity of the document.

b. The DON will enable DON information systems to use Public Key Infrastructure (PKI) for digital signature and encryption in accordance with reference (a). DON digital signatures shall only rely on certificates issued by the DoD PKI or by a DoD-approved PKI for authentication, digital signature, or encryption. External PKIs must be approved for use by the DoD CIO.

5. Responsibilities. Organizations with applications, systems, and business processes that use digital signatures shall comply with references (a) through (e) and the following:

a. Consider contingency, work-around, or back-up signature procedures for any processes that rely upon the use of digital signatures.

b. 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.

c. Enable a digitally signed document to be converted to a paper copy as required or needed. Any converted paper document shall indicate that the document was digitally signed. When the digital signature information is required or requested for records management or legal purposes, the paper copy shall minimally contain:

(1) A statement or other indication that the document or form was digitally signed;

(2) Name of the individual who digitally signed the document or form;

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

(4) Date and time document was signed; and

(5) Ensure the integrity of digitally 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.

6. Background

a. Reducing DON 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 digital signatures, when practicable, is essential to the DON complying with DoD and Federal Government requirements for paperless processing. References (a) through (e) provide digital signature policy and requirements for DoD and the Federal government.

b. Consistent with reference (a), a “digital signature” is a method of authenticating records by producing a signature bound to both the record and the signer’s identity using cryptographic keys, operations, and protocols. A digital signature is produced by a user’s computer using a PKI certificate, typically via a Common Access Card through an asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection.

7. Records Management

a. Records created as a result of this instruction, regardless of format or media, must be maintained and dispositioned according to the records disposition schedules found on the Directives and Records Management Division (DRMD) portal page: https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/SitePages/Home.aspx.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local Records Manager or the DRMD program office.

THOMAS B. MODLY
Under Secretary of the Navy

Distribution:
Electronic only, via Department of the Navy Issuances website https://www.secnav.navy.mil/doni/.