U.S. Department of Commerce
Digital Signature Policy

Version 1.0

Purpose
This policy establishes the adoption and use of digital signatures as legally binding and the standard business practice for all Department of Commerce internal processes that require digital signatures.

Authorities:

- The Government Paperwork Elimination Act 2003 (USC Title 44 Chapter 35-04),
- The Electronic Signatures in Global and National Commerce Act (2000) (USC Title 15 Chapter 96)
- The Uniform Electronic Transactions Act (1999)
- OMB Memorandum M-0524

Definitions

- **Digital Signature** – The term used to describe the small segment of data produced when a specific mathematical process (involving a hash algorithm and public key cryptography) is applied to an electronic record. Also known as an advanced, standard, or secure electronic signature, digital signatures are based on Public Key Infrastructure (PKI) technology and are commonly used to verify the integrity and authenticity of software, email, or financial transactions, and other scenarios in which it is important to detect forgery or tampering.
- **Electronic Record** – A document, form, or other record created, generated, sent, communicated, received, or stored by electronic means.
- **Legally Binding Electronic Signature** – Where an electronic signature is required or otherwise deemed desirable, it is critical that the electronic signature and the associated signing process satisfy all of the applicable legal requirements.
- **PIV Card** - A personal identity verification card (PIV card) is a specific type of smart card technology that allows individuals to gain access to U.S. federal resources and facilities.
- **Signing Process** – The set of actions, steps, and elements used to create a legally binding electronic signature including application of an electronic form of signature to an electronic record and one or more processes or security procedures to address the other signature requirements of a legally binding signature, including identifying and authenticating the signer and ensuring integrity of the electronic record.

Scope
This policy is applicable to all forms, documents, agreements, and transactions produced and/or conducted electronically within the Department of Commerce. This policy applies to all employees of the Department of Commerce, employees of other federal agencies on detail to the Department, and anyone else utilizing any information technology (IT) infrastructure owned or operated by the Department or its operating units.

Policy
This policy establishes the requirements for the adoption and use of digital signatures as a standard business practice for all Department of Commerce internal business processes that require a signature.

Digital Signatures must be accomplished using the credentials on the Personal Identity Verification (PIV II) card or other approved smart identity card issued by the Department.

The use of digital signatures must comply with all other existing laws, regulations, and policies, as well as guidance from the National Archives and Records Administration on the use of digital signatures in records management (*see references below*).

Guidance
Each user of the Department's IT infrastructure, when issued a PIV II card, has the necessary certificates to execute a digital signature. The certificates are used in the authentication process performed by the certificate authority (CA) to validate the signature. The PIV II card (or equivalent as noted above) will be the only approved source of certificates used in conjunction with this policy.

In accordance with this policy, digital signatures will be accepted as valid for all internal Departmental documents. The capability to use digital signatures with agencies outside of the Department must be validated with the receiving agency prior to signing a document. This policy is not a mandate to replace "wet signatures" but rather to authorize the use of digital signatures as the preferred means of conducting business transactions within the Department.

PIV Card Usage and Privacy Act Notice
Common to all federal agencies, the PIV card is a way for you to prove that you are who you claim to be[1]. PIV cards are issued to reduce identity fraud, protect your privacy, save time, and improve security through a standardized process. As part of this process, the U.S. Government conducts a BI on you to decide whether you are suitable for your job and eligible to use the buildings, computers, applications and data you need to do your job. Some of the information you provide for your BI, along with information from the office that hired you, is used to verify your identity, create a PIV card for you, and create a record that you have been issued a card[2].

The Departmental Privacy Act regulation requirements on safeguarding Privacy Act information must be used to ensure that appropriate safeguards are in place for handling PIV information (refer to 43 CFR 2.51 and 383 DM 8).

References
The laws governing electronic signatures and official policy are outlined in:

- The Government Paperwork Elimination Act 2003 (USC Title 44 Chapter 35-04),

[1] *OMB Memorandum M-05-24*
[2] *HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors*

- The Electronic Signatures in Global and National Commerce Act (2000) (USC Title 15 Chapter 96)
- The Uniform Electronic Transactions Act (1999)
- Office of Management and Budget (OMB) Memorandum M-00-15 OMB “Guidance on Implementing the Electronic Signatures”
- OMB Memorandum M-00-10 OMB “Procedures and Guidance on Implementing the Government Paperwork Elimination Act”

Technical Requirements and Standards are defined in:

- National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication 186-4 (FIPS PUB 186-4) “Digital Signature Algorithm Validation System”
- NIST Federal Information Processing Standards Publication 201-2 (FIPS PUB 201-2) Personal Identity Verification (PIV) of Federal Employees and Contractors” ,)
- NIST Special Publication 800-85B-4”PIV Data Model Test Guidelines”
- NIST Special Publication 800-73-4 “Interfaces for Personal Identity Verification”

Records Management Requirements and Guidance:

- Revised Format Guidance for the Transfer of Permanent Electronic Records, NARA Bulletin 2014-04:

This policy is supplemental to a suite of security controls consisting of:

- Commerce Information Technology Requirements;
- DOC Information Technology Security Program Policy (ITSPP);
- NIST Special Publication 800-53, “Security and Privacy Controls for Federal Information Systems and Organizations;”
- National Archives and Records Administration (NARA) Transmittal 23 part GRS 3.2 items 060-062;

Additional Supporting information:

- "Use Of Electronic Signatures In Federal Organization Transactions" US Federal CIO Council, Version 2.0 January 25, 2013

Background

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital message or document. A valid digital signature gives a recipient assurance that the message or document was created by a known sender, such that the sender cannot deny having sent the message and that the message was not altered in transit. The encrypted data constituting the digital signature can be applied as a legally binding signature, provided it is used in a manner that satisfies all of the requirements for a legally binding electronic signature. Electronic signatures must be functionally equivalent to the signature applied to a paper record. The goal is to specify criteria which, once met by a digital signature, enable the signature to have the same level of legal recognition as a corresponding handwritten signature without imposing more stringent standards of security. To be functionally equivalent to a handwritten signature, the E-Transaction laws require that the electronic form of signature

must be made part of the record being signed (i.e., being attached to or logically associated with the record being signed).

For Additional Information:
For technical assistance, contact your local help desk or IT Security Officer (ITSO)
For records management issues contact your records management officer
For PIV Card Training, please contact the Office of Security (OCS)

Appendices and Job Aids:

- How to Digitally Sign a Performance Plan
- Security Practices for Electronic Mail
- Saving a Digitally Signed Document as a Smaller File Size
- Electronic Authentication Guideline (NIST Special Publication 800-63-2)

Forms Prescribed:

- **Department of Commerce Personal Identity Verification (PIV) Request**
  Form #: CD-591
  (*http://ocio.os.doc.gov/s/groups/public/@doc/@os/@ocio/@oitpp/documents/content/dev01_002580.pdf*)

- **Sensitive Information Cover Sheet**
  Form#: CD-494
  (http://ocio.os.doc.gov/s/groups/public/@doc/@os/@ocio/@oitpp/documents/content/prod01_003118.pdf)

Approved and Issued By:

STEVEN COOPER

Digitally signed by STEVEN COOPER
DN: c=US, o=U.S. Government, ou=Department of Commerce, ou=Office of the Secretary, cn=STEVEN COOPER, 0.9.2342.19200300.100.1.1=13001003023093
Date: 2016.11.03 18:43:08 -04'00'

Steve I. Cooper, Chief Information Officer
Office of the Chief Information Officer, (OCIO)
Department of Commerce

Date: November 3, 2016

Projected Document Review Date*: NLT April 3, 2017

** Revision date should not exceed 3 years past date of issuance.*