Records Management Policy: RMP-2020-01

Subject: Digital Signature Usage in Records

1. Effective Date:

This policy is effective as of **June 8, 2021**.

2. Version:

Version #	Description	Comment
1.0	Initial Policy	Initial Policy Issued

3. Rescissions: None

4. Prepared By:

A. Regina A. Wendling, IT Program Manager, Office of the Chief Information Officer, September 2, 2020

B. Christina Bartlett, Chief, Information Management Branch, U.S. Geological Survey, September 17, 2020

5. Purpose

This policy outlines the U.S. Department of the Interior's (Department) standard and guidelines for signing electronic documents with digital signatures. A digital signature provides a high-levelof assurance that the claimed signatory signed the electronic document. Documents that traditionally require notarization or wet-ink signatures require this level of assurance.

6. Scope

Agencies should use digital signatures for documents that require high levels of assurance or for convenience in lower-risk electronic documentation. This policy focuses on the use of digital signatures to provide higher levels of assurance and trustworthy records.

7. Authorities

A. 15 U.S.C. Chapter 96, Electronic Signatures in Global and National Commerce Act
B. Public Law 105-277 Sections 1703-1710, Government Paperwork Elimination Act (GPEA) (44 U.S.C. Section 3504 note)
C. Public Law 115-336 21st Century Integrated Digital Experience Act (IDEA)
D. Office of Management and Budget (OMB) Memorandum M-19-21 – Transition to Electronic Records
E. National Institute of Standards and Technology (NIST) Special Publication 800-63-3 – Digital Identity Guidelines
F. Federal Information Processing Standards (FIPS) 186-4 – Digital Signature Standard (DSS)

G. National Archives and Records Administration Bulletin 2015-03, Guidance on Managing Digital Identity Authentication Records
H. Office of the Chief Information Officer (OCIO) Directive 2020-003 – Digital Signature Policy

8. Policy

A. The Department's digital signature standard is comprised of using the "DOI Access Card," also known as the Personal Identity Verification (PIV) Card, to apply digital signatures as the authorized digital signature method. The Department will apply this standard as outlined below.

1. Internally – Using Digital Signatures within the Department. The Department requires Departmental Staff to use authorized digital signature methods to electronically sign documents involving transactions that require high levels of assurance, such as agreements and forms involving funds, contracts, or other documents that commit the Department to some form of legal liability.

2. Externally – Using Digital Signatures with External Organizations. Departmental Staff may use authorized digital signature methods to electronically sign documents and forms with non-federal government organizations contingent on the recipient's acceptance of this format. Departmental Staff may not require non-federal government organizations or individuals to accept or use digital signatures; therefore,they must accommodate the use of wet-ink or notarized signatures as appropriate when an external recipient rejects the digital signature.

3. Exceptions. This policy does not require the use of digital signatures for low assurance transactions, documents, and forms; therefore, current electronic signature practices (e.g., using government e-mail messages) remain acceptable. Alternative digital signature methods may be acceptable upon approval from your respective Associate Chief Information Officer (ACIO) and Office of the Solicitor.

B. Bureaus and offices may not use unauthorized or inappropriate digital or electronic signature methods. Bureaus and offices currently using alternative electronic approval/signature processes must complete a risk assessment within 90 days of the Department's Digital Signature Policy effective date and obtain approval from the respective ACIO and the Office of the Solicitor. If the risk assessment shows an unacceptable level of risk, the bureau or office must develop a plan of action and milestones to update the process to an approved method with an acceptable level of risk.

9. Responsibilities

A. OCIO/ACIO will authorize the use of alternative methods to PIV digital signature usage that meet all laws, regulations, and legal requirements.

B. Departmental Staff must:

1. complete a risk assessment and collaborate with the appropriate offices and staff (e.g., Responsible Records Officer, Privacy Officer, Office of the Solicitor) todetermine the appropriate electronic/digital signature needed based on the identity assurance level for the document.

2. obtain prior approval or concurrence by non-federal government organizations or

individuals for use of digital signatures instead of a wet-ink, handwritten signature.

3. obtain Office of the Solicitor and ACIO approval for alternative methods to PIVdigital signature usage prior to use or implementation.