INFORMATION DIRECTIVE
POLICY

Electronic Signature Policy		
Directive No.: CIO 2136.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

Electronic Signature Policy

1. PURPOSE

This policy establishes the United States (U.S.) Environmental Protection Agency's (EPA) approach for adopting electronic signature technology and best practices to ensure electronic signatures applied to official Agency documents are legally valid and enforceable.

2. SCOPE

The policy formalizes and standardizes EPA's electronic signature policy for internal Agency processes. It applies to all internal Agency processes that are adopting and implementing electronic signature technologies to sign Agency electronic records. EPA policies as well as external federal mandates drive the scope of the requirements with which electronic signature implementations must comply. For example, Federal Information Security Modernization Act (FISMA)/Federal Information Processing Standards (FIPS), Privacy Act, Federal Acquisition Regulations (FAR) and records management requirements define security, legal, and records retention requirements for electronic signature implementations.

Requirements for complying with EPA's Cross-Media Electronic Reporting Rule (CROMERR) are driven by Title 40 of the Code of Federal Regulations (CFR) Part 3 and are referenced as best practices for a robust electronic signature implementation. Offices must consult with their Information Security Officer (ISO), the Office of General Counsel (OGC) and Records Liaison Officers (RLOs) to ensure their electronic signature process meets security, legal, records management and other business requirements.

This policy applies to new uses of electronic signature technology. Existing electronic signature implementations that were developed prior to the approval date of this policy will be grandfathered, as long as applicable requirements (i.e., FISMA/FIPS, Privacy Act, Records Management) are met by the existing implementation. System owners must adopt the requirements of this policy in any future major upgrades or modernization efforts. While this policy does not mandate use of a specific technology, the technology selected must comply with the FISMA/FIPS and the Privacy Act. Offices may use any valid electronic signature solution that meets its business requirements so long as it also complies with FISMA/FIPS and the Privacy Act for its implementation. This includes using FIPS 140 lab certified cryptographic modules (i.e., Microsoft Office uses Microsoft Cryptographic Application Programming Interface (MS-CAPI); Adobe Sign uses RSA BSAFE Crypto-C).

Electronic Signature Policy		
Directive No.: CIO 2136.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

3. AUDIENCE

The audience includes all EPA employees, contractors, grantees and other authorized agents who need to sign records (i.e., documents, forms, correspondence, and/or emails) in support of EPA business and administrative operations. Signers must have approved EPA credentials that conform to the EPA Information Technology (IT) Architecture Standards Profile.

4. BACKGROUND

The Electronic Signatures in Global and National Commerce Act (E-Sign Act)[1] and Office of Management and Budget (OMB) and the National Archives and Records Administration (NARA) Directive M-12-18: Managing Government Records[2], provide the foundation and requirements for EPA's Electronic Signature Policy, Procedure and associated Guidance. The E-Sign Act clarifies that electronic signatures are legally valid and enforceable under United States law. Directive M-12-18 mandates that, "by December 31, 2019, all permanent electronic records in Federal agencies will be managed electronically to the fullest extent possible for eventual transfer and accessioning by NARA in an electronic format."

Electronic signature technology supports these requirements and is used to authenticate identity and to verify the integrity of signed electronic records. Electronic signatures document the signer's intent, provide evidence that a specific individual signed the electronic record, and maintain an electronic record of the signature that cannot be changed without detection.

5. AUTHORITY

- Office of Management and Budget (OMB) and the National Archives and Records Administration (NARA), Managing Government Records Directive (M-12-18) (August 24, 2012). https://www.archives.gov/files/records-mgmt/m-12-18.pdf
- Electronic Signatures in Global and National Commerce Act (E-SIGN Act), Public Law 106-229 (June 30, 2000). https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf

6. POLICY

Many internal Agency processes require EPA employees, contractors, grantees and other authorized agents to sign documents in order to signify knowledge, approval, acceptance, obligation, or intent by the identified signatory. Use of electronic signature technology will

[1] • *Electronic Signatures in Global and National Commerce Act (ESIGN Act), Public Law 106-229 (June 30, 2000).*

[2] • *Office of Management and Budget (OMB) and the National Archives and Records Administration (NARA), Managing Government Records Directive (M-12-18) (August 24, 2012).*

result in reductions in costs and other business efficiencies. This policy identifies the following objectives that EPA will meet to standardize its approach for electronic signature:

1. Integrate and standardize the electronic signature process as part of the records life cycle while leveraging investments in existing Agency records management systems.
2. Align with federal cryptographic and record keeping requirements and EPA electronic reporting requirements (i.e., those specified by FISMA, Privacy Act, NARA, 40 CFR Part 3. See Section 8).
3. Support the transition of official processes that generate "paper" official records to electronic records by providing a set of criteria and processes for legally acceptable electronic signature implementation and promoting the use of electronic storage systems.
4. Introduce efficiencies into Agency-wide and office-specific processes and workflows.
5. Ensure electronic signature implementations meet the legal equivalency of existing "wet ink" signature in terms of preserving civil and criminal enforceability in court proceedings.

Within eighteen months of the implementation of this policy, offices should evaluate their paper-based processes to identify those which are good business cases for migrating to electronic signature processes. For those where there is a good case, the office should prioritize those and pursue migrations as resources permit. Once implemented, the resulting signed documents, forms, correspondence and/or emails shall be managed according to the appropriate information directives for Agency records.

7. ROLES AND RESPONSIBILITIES

- **The Chief Information Officer (CIO)** facilitates the process for appropriate business organizations to incorporate the Electronic Signature Policy into their organization and operations.
- **Senior Information Officials (SIOs)** implement Electronic Signature Policy, Procedure, and Guidance, and approve the use of electronic signature capabilities within their program and regional offices.
- **Information Management Officers (IMOs)/Regional Information Resources Management Branch Chiefs (IRM BCs)** advise the SIOs on implementing Electronic Signature processes within their program and regional offices and ensure processes and systems that use electronic signature capabilities comply with this Policy, Procedure and Guidance.
- **Information Security Officers (ISOs)** ensure that systems that use electronic signature capabilities comply with this Policy, Procedure, and Guidance as well as other security requirements.
- **Records Liaison Officers (RLOs)** participate in the development and maintenance of electronic signature standards and procedures, as appropriate, for relevant programs, regional offices, laboratories, etc. and support and implement standards, technical specifications, the Procedure, and standard operating procedures (SOPs) for their organizations by doing the following:

  - Work with records, document and content owners/generators to plan and manage the life cycle of the electronically signed records.
  - Assist employees and other agents who require electronic signature capabilities to implement the Policy, Procedure and Guidance.
  - Coordinate with the IMO/IRM BC, and provide outreach, support, and technical assistance as appropriate to ensure the proper implementation of the Policy, Procedure and Guidance.
- **Records Custodians** use the Procedures to capture Agency-owned electronically signed records.
- **Contracting Officer Representatives (CORs)**, instruct contractors to employ the Procedure and Guidance in signature processes.
- **System Owners** adopt the requirements of EPA's Electronic Signature Policy, Procedure and associated Guidance in electronic signature implementations.

8. RELATED INFORMATION

- NARA/Records Management Guidance and Regulations https://www.archives.gov/records-mgmt/policy/guidance-regulations.html
- U.S. EPA Electronic Signature Procedure (April 2018) https://www.epa.gov/sites/production/files/2018-04/documents/electronic_signature_procedure.pdf
- U.S. EPA eReporting Policy Memorandum (September 2013) https://www.epa.gov/sites/production/files/2016-03/documents/epa-ereporting-policy-statement-2013-09-30.pdf
- U.S. EPA Information Technology (IT) Architecture Standards Profile http://cfint.rtpnc.epa.gov/oito/itarchitecture/standards.cfm
- CIO 2155.3: U.S. EPA Records Management Policy (February 2015) https://www.epa.gov/sites/production/files/2015-03/documents/cio-2155.3.pdf
- CIO 2122-P-01.1: U.S. EPA Enterprise Architecture Governance Procedures (November 2012) http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/CIO-2122-P-01.1.pdf
- National Institute of Standards and Technology (NIST), Minimum Security Requirements for Federal Information and Information Systems (FIPS 200) (March 2006). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
- NIST, Security Requirements for Cryptographic Modules (FIPS 140-2) (August 2013) https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

Electronic Signature Policy		
Directive No.: CIO 2136.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

- NIST, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths (NIST SP 800-131A Revision 1) (November 2015). https://csrc.nist.gov/publications/detail/sp/800-131a/rev-1/final

- NIST, Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS 201-2) (August 2013). https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

- Homeland Security Presidential Directive 12 (HSPD-12) – Policy for a Common Identification Standard for Federal Employees and Contractors (August 2005) https://www.dhs.gov/homeland-security-presidential-directive-12

- OMB M-11-11 Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors (PDF, February 2011) https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf

- OMB M-05-24 Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors (PDF, August 2005) https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2005/m05-24.pdf

- NIST Special Publication 800-63-3 – Digital Identity Guideline (May 2017) https://pages.nist.gov/800-63-3/sp800-63-3.html

- NIST Special Publication-800-63-2 Electronic Authentication Guideline (PDF, August 2013) https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

- OMB M-04-04 E-Authentication Guidance for Federal Agencies (PDF, December 2003) https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2004/m04-04.pdf

- Executive Order 13681 Improving the Security of Consumer Financial Transactions (October 2014) https://obamawhitehouse.archives.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions

- OMB Memorandum for Chief Information Officers of Executive Departments and Agencies: Requirements for Accepting Externally-Issued Identity Credentials (October 6, 2011) https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/egov_docs/ombreqforacceptingexternally_issuedidcred10-6-2011.pdf

- U.S. EPA Code of Federal Regulations. Title 40. Part 3. Cross-Media Electronic Reporting (CROMERR) (October 2005) https://www.ecfr.gov/cgi-bin/text-idx?SID=0245de321adebd80c389f68ae30e1415&mc=true&node=pt40.1.3&rgn=div5

Electronic Signature Policy		
Directive No.: CIO 2136.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

9. DEFINITIONS

- **Digital Signature** – A subset of electronic signature technology. Digital signatures encrypt documents with digital codes to verify the user's identity and support authentication, data integrity and signer non-repudiation. Electronic signature technologies must comply with FIPS 180-4 Hash (https://csrc.nist.gov/publications/detail/fips/180/4/final) and FIPS 186-4 (https://csrc.nist.gov/publications/detail/fips/186/4/final) Digital Signature standards.
- **Electronic Signatures** – Legal concept that uses technology to ensure the signature may not be denied legal effect, validity or enforceability.
- **Non-Repudiation** – Assurance that the signer cannot deny the authenticity of their signature.
- **Personal Identity Verification (PIV) Card** – Identity credentials issued by the Federal government to its employees and contractors that are used to authenticate individuals who require access to federally owned systems. (See FIPS PUB 201-2 (https://csrc.nist.gov/publications/detail/fips/201/2/final) controlled facilities, information systems, and applications.
- **Public Key Certificate** – A set of data that uniquely identifies a public and private key pair needed to compute an electronic signature and the owner that is authorized to use the key pair. The certificate contains the owner's public key and is electronically signed by the issuing certification authority, i.e., a trusted party, thereby binding the public key certificate to the owner. The private key, known only to the owner, is used to compute the electronic signature; the public key can be shared and is used to verify the electronic signature.

10. WAIVERS

N/A

11. MATERIAL SUPERSEDED

N/A

12. CONTACTS

For further information about the policy, please contact the EPA Office of Environmental Information, Office of Information Management.

Steven Fine
Principal Deputy Assistant Administrator for Environmental Information
and Deputy Chief Information Officer
U.S. Environmental Protection Agency

Electronic Signature Policy		
Directive No.: CIO 2136.0	CIO Approval: 4-30-2018	Transmittal No.: 18-005

APPENDIX

ACRONYMS & ABBREVIATIONS

CFR – Code of Federal Regulations
CIO – Chief Information Officer
COR – Contracting Officer Representative
CROMERR – Cross-Media Electronic Reporting Rule
EPA – U.S. Environmental Protection Agency
ESIGN – Electronic Signatures in Global and National Commerce Act
FAR – Federal Acquisition Regulations
FIPS – Federal Information Processing Standards
FISMA – Federal Information Security Modernization Act
IMO – Information Management Officer
IRM BC – Information Resources Management Branch Chief
ISO – Information Security Officer
IT – Information Technology
NARA – National Archives and Records Administration
NIST – National Institute of Standards and Technology (NIST)
OGC – Office of General Counsel
OMB – Office of Management and Budget
PIV – Personal Identity Verification
RLO – Records Liaison Officer
SIO – Senior Information Officer
SOP – Standard Operating Procedure