Homeland Security

Electronic Signature Use, Acceptance, and Implementation Guidance

Version 1.0

March 21, 2022

This page intentionally blank.

Document Change History

Version	Date	Description
1.0	March 21, 2022	Initial Draft

TABLE OF CONTENTS

1.0 INTRODUCTION

This guidance document identifies the specific processes and requirements supporting the use, acceptance, and implementation of electronic signatures within the Department. Although digital signatures are a form of electronic signature, they are covered in greater detail within the DHS Sensitive Systems Policy Directive 4300A and supportive documentation.

2.0 SCOPE

This guidance document applies to all internal and external Departmental processes that implement electronic signatures technologies to allow individuals to sign, attest, or acknowledge electronic records.

3.0 RESPONSIBILITIES

1. **DHS Chief Information Officer (DHS CIO)** provides oversight and advises Components, to include Component Chief Information Officers, and the DHS Chief Information Security Officer (CISO) when implementing this guidance. Focuses on improving the user experiences of external parties who conduct business with the Department by implementing standards for collecting electronic signatures. Coordinates with the DHS Office of the General Counsel (OGC), and relevant Component Counsel(s), to eliminate duplicate electronic signature requirements, as appropriate.

2. **Component Chief Information Officers (CIOs)** implement this guidance pursuant to governing laws, regulations, and electronic signature policy and guidance in their organization and operations. Approves use of electronic signatures within their program, and operations in coordination with the DHS OGC and relevant Component Counsel(s). Approves the design, development, and infrastructure for implementation of electronic signatures using digital signatures or other electronic signature methods.

3. **DHS Chief Information Security Officer (CISO)** ensures that all systems that employ electronic signature capabilities comply with the governing laws, regulations, this policy guidance, as well as other security measures required by statute, regulation, and policy.

4. **Component Chief Information Security Officers (CISOs)** ensure that systems within their Component that employ electronic signature capabilities comply with governing laws, regulations, and this guidance as well as other security measures required by statute, regulation, and policy.

5. **Component Chief Records Officers** participate, as stakeholders, in the development, implementation, support, and maintenance of electronic signature standards, technical specifications, and procedures as related to records management, for relevant programs and offices within their Component by:

    (a) Planning and managing the lifecycle of electronically signed records (For the purposes of this guidance, the terms "document" and "record" shall have the same meaning as found in the Federal Records Act (FRA), 44 U.S.C. § 2101 et.seq., and the Electronic Signatures in Global and National Commerce Act (E-Sign Act), 15 U.S.C. § 7001 et.seq., with record and document generators and owners.)

    (b) Assisting employees and other agents as related to records management, who require electronic signature capabilities to implement the Guidance.

(c) Coordinating with Component CIOs to provide outreach, support, and technical assistance to ensure the proper implementation of this guidance as related to records management functions.

6. Component Legal Counsel

(a) For their Component, advises on when implementing an electronic signature collection program to ensure all transactions signed, attested, or acknowledged with electronic signatures are recorded and maintained in accordance with all applicable statutes, regulations, and policies.

(b) For their Component, assesses the legal sufficiency of electronic signatures for internal, incoming, and outgoing transactions, operational purposes, and communications. Determines the acceptability and validity of submissions of electronically signed documents or records from third parties and externally generated material that is electronically signed.

(c) Participates in inter-agency coordination with the relevant Department of Justice components and other federal agencies to help ensure that their equities, including utilization of electronically signed documents in criminal prosecutions and civil litigation as appropriate, are satisfactorily protected, attested, or acknowledged by an electronic signature.

(d) For their Component, assesses the legal sufficiency of policies, procedures, and set forth the legal standards for determining the legal sufficiency of electronically signed documents (in coordination with the relevant Department of Justice components when appropriate), maintenance and retention of electronically signed documents for chain of custody purposes, and storage and disposal of electronically signed records in the agency's custody.

(e) For their Component, reviews and advises on the legal sufficiency of policy and guidance related to electronic signature collection, acceptance, use, and retention.

7. **System Owners** adopt the requirements of this Guidance when implementing electronic signature collection program.

8. **DHS Office of the General Counsel (OGC)**

(a) For the Department, advises on when implementing an electronic signature collection program to ensure all transactions signed, attested, or acknowledged with electronic signatures are recorded and maintained in accordance with all applicable statutes, regulations, and policies.

(b) For the Department, assesses the legal sufficiency of electronic signatures for internal, incoming, and outgoing transactions, operational purposes, and communications. Determines the acceptability and validity of submissions of electronically signed documents or records from third parties and externally generated material that is electronically signed.

(c) Participates in inter-agency coordination with the relevant Department of Justice components and other federal agencies to help ensure that their equities, including utilization of electronically signed documents in criminal prosecutions and civil litigation as appropriate, are satisfactorily protected, attested, or acknowledged by an electronic signature.

(d) For the Department, assesses the legal sufficiency of policies, procedures, and set forth the legal standards for determining the legal sufficiency of electronically signed documents (in coordination with the relevant Department of Justice components when appropriate), maintenance and retention of electronically signed documents for chain of custody purposes, and storage and disposal of electronically signed records in the agency's custody.

(e) For the Department, reviews and advises on the legal sufficiency of policy and guidance related to electronic signature collection, acceptance, use, and retention

4.0 Requirements

The Electronic Signatures in Global and National Commerce Act[1] defines an electronic signature as "[a]n electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[2]An electronic signature is used for the same purpose as a handwritten signature, or any other form of signature currently accepted or approved by the Department. A properly executed and authenticated electronic signature must possess the same qualities and attributes that guarantee a handwritten signature's authenticity. An electronic signature records the signer's intent and , provides legally sufficient evidence that a specific individual signed the electronic record,

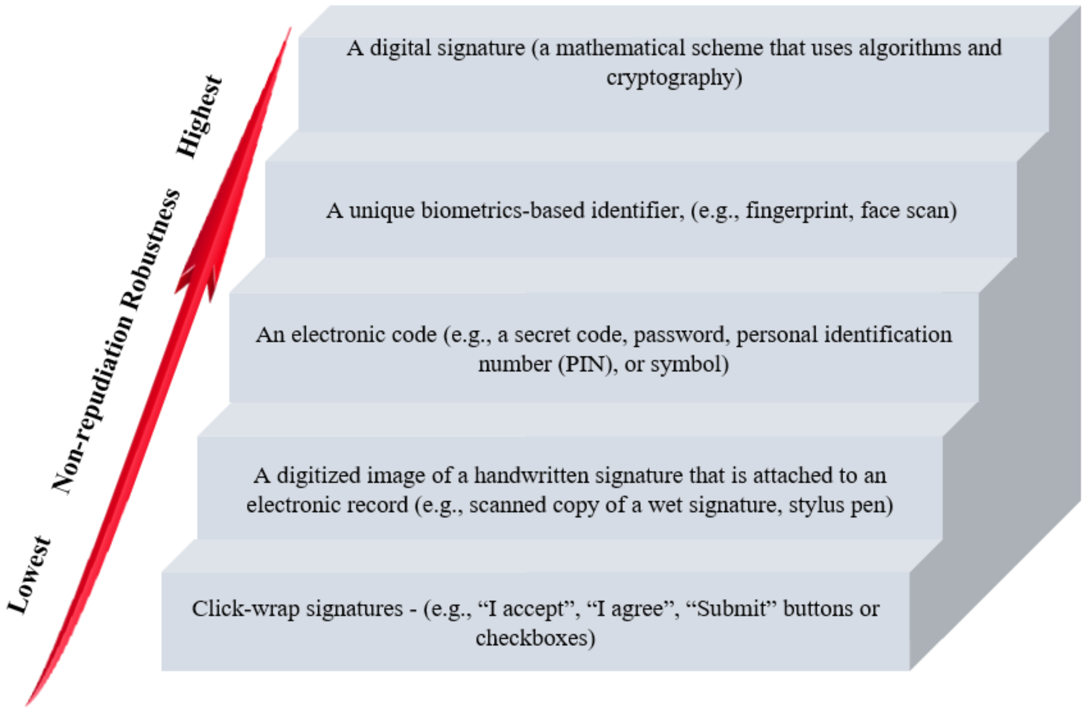
Electronic signatures may appear in various forms or in combinations of types. However, all electronic signatures must comply with legal requirements for electronic, signature collection, including the need to implement an appropriate non-repudiation safeguard for the signature. Per DHS policy as enumerated here, this safeguard, as implemented through the type of signature, should be based upon the nature of the transaction and the document being signed.

Common electronic signature formats are depicted in Figure 1 below and ordered from lowest to highest level of non-repudiation protection:

[1] Pub. L. No. 106-229 (2000)

[2] 15 U.S.C. § 7006(5).

Figure 1: Examples of Electronic Signatures


Highest
Non-repudiation Robustness
Lowest
A digital signature (a mathematical scheme that uses algorithms and cryptography)
A unique biometrics-based identifier, (e.g., fingerprint, face scan)
An electronic code (e.g., a secret code, password, personal identification number (PIN), or symbol)
A digitized image of a handwritten signature that is attached to an electronic record (e.g., scanned copy of a wet signature, stylus pen)
Click-wrap signatures - (e.g., “I accept”, “I agree”, “Submit” buttons or checkboxes)

The type of electronic signature used for a specific agency transaction should be based on the nature of the transaction and the purpose for which the electronic signature will be used. Appendix A, “Determining Which Electronic Signature Method to Use - Risk Assessment and Cost-Benefit Analysis,” provides a methodology for determining the electronic signature method to use based on a risk assessment and cost-benefit analysis.

If the electronic signature is collected in a transaction that does not impose or affect any contractual or legal obligations (.e.g., agreeing to participate in an anonymous survey or accepting an invitation to a voluntary event with no legal consequences for failure to appear), then a low-level electronic signature, such as a click-wrap signature, may suffice.

If the electronic signature will be used in a court of law to establish the identity or authenticate the signer (e.g., signing a form to obtain a permanent benefit from the U.S. Government) or establish the signer’s intent to execute a specific legally enforceable transaction (e.g., a signature accepting legal service of process), then it may be appropriate to implement higher-level electronic signatures, such as a digital signature or a biometric-based signature, to provide the greatest degree of non-repudiation.

When implementing electronic signatures accepted from an external party for a specific use that requires a high degree of non-repudiation, signature collection using a unique biometric-based identifier is preferred, unless the signers can use a Personal Identity Verification (PIV) Card, DoD-issued Common Access Card (CAC), Personal Identity Verification – Interoperable (PIV-I) Card, or software-based Digital Signature certificate meeting the requirements specified in the DHS Electronic Signature Policy Guidance document, version 1.01, Section III. Policy Statement DS.1. Among biometric identifiers, DHS prefers to utilize fingerprints as a non-repudiation measure for high-risk transactions where there is a higher-level need of non-repudiation.

4.1 Component Electronic Signature Criteria

Electronic signatures must meet the following basic criteria to be considered valid:

1. *Uniqueness*. The signature must be unique (a means to identify the signature from other signatures) to the signatory based on the non-repudiation robustness determined and required for the article being signed. For high-level non-repudiation requirements, the electronic signature is only acceptable if it is distinctively identifiable as that of the individual signer. A unique signature should identify a specific individual and be difficult to duplicate. For low-level non-repudiation requirements, the electronic signature must distinctively identify the signing action from other signing actions.

2. *Control*. For signatures requiring high-level non-repudiation, the electronic signature must be under the sole control or attribution of the signer. This can be accomplished using various techniques such as biometrics to log into a system, multi-factor authentication methods, the PIV card, or other means to access a system and affix the signature to ensure that only the specific signer can use the electronic signature being applied. In cases where the signer is required to access a system, the capability used to affix the electronic signature must still be under the sole control of the signer such as a PIV card, token, biometric or other means to ensure that only the authorized individual accessed and applied the electronic signature.

3. *Intent to Sign*. The system must display an electronic signature block or identify to the signer that they are signing a record. The signature block or signature identification method must contain a word or statement that definitively conveys the signer's intent to affix his or her signature to the associated record and to give them the opportunity to review the document and make any changes or corrections before the signature is affixed. Methods can vary depending on the non-repudiation requirements. Examples of statements that convey the signer's intent include, but are not limited to:

- "Validated by"
- "Signed by"
- "Certified by"
- "Instructor's signature/certification"
- "Signature"
- "Authorized by"
- "Signatory"
- "Authentication"
- "Acknowledged by"
- "Acknowledgement" and/or
- "Affirmed by"
- "Agreed to by"

The signer must know exactly what they are attesting to or acknowledging prior to electronically signing the record. A valid electronic signature is only enforceable for content the signer is allowed to review prior to signing the record. Components should work with DHS OGC or Component Counsel(s) to determine if additional requirements exist (e.g., a check box indicating that translation services have been offered for populations that do not speak English as a first language) to ensure the signer understands the content of the document or record being signed.

4. *Deliberate*. An individual who electronically signs a document must take a deliberate and recognizable action to affix their signature. Acceptable deliberate actions for creating an electronic signature include, but are not limited to, the following:

- Executing a digital signature
- Entering a unique code (note an individual's information technology system username and password must not be used for electronic signature execution)
- Swiping a badge
- Signing a signature pad, tablet, or other electronic device with an electronic stylus or other signing capability
- Providing a unique biometric identifier
- Clicking a button or typing words, including a name.

5. *Signature Association*. A valid electronic signature must be attached to, or logically associated with, the record being signed.

The electronic signature applied by the signer must be linked to the record being signed. Satisfying this requirement requires that the electronic signature, and associated data, are permanently linked with the electronic record that was signed and protects it from alteration.

6. *Notification*. The system should notify or identify to the signer that his or her signature has been affixed to the record or provide confirmation of the signing action based on the specific non-repudiation requirements.

4.2 Component Electronic Signature Process

Each Component's electronic signature collection process must use certain standard practices, IT security capabilities, and the collection and retention of specific data necessary to render the electronic signature legally enforceable. When applicable, the electronic signature collection system must concurrently capture the date and time that the record was signed, the identification information of the signer, the signer's intent to sign, and the signer's express adoption of the contents as true and correct, and that the document was signed under penalty of perjury where appropriate. The signing system and process must also create and store the particular record, ensuring the electronic signature is attached to or associated with the record, and must detect any alteration of the record after signature. Once a record has been electronically signed, any modification must be supported by collection of a new electronic signature. In cases where additional signatures are required, adding the additional signatures does not void the initial signature, or require the initial signer to re-sign. The electronic signature collection process is product-specific, so Components must ensure that the form of electronic signature chosen adequately maintains the integrity of the record. Component electronic signature processes should describe, contain, or address the following:

1. *Retrievable and Traceable*. The signer should be able to identify, retrieve or receive a copy of documents he or she has electronically signed and, at minimum, be provided either an electronic

or hardcopy version of the electronically signed document when specifically required by law or policy

2. *Non-Repudiation Strength*. A person[3] (the signer) must use an acceptable form of electronic signature. The type of electronic signature should be based on the noon-repudiation safeguards needed for the document at issue. An electronic signature collection process must contain procedures and security controls that ensure the authenticity of the signature, the identity of the signer, and the signer's intent to sign the particular record. When determining appropriate non-repudiation safeguards for specific electronic signature collection processes, Components should work with the DHS OGC or Component Counsel(s), as appropriate, to determine repudiation risks and whether additional authentication measures (e.g., simultaneous collection of electronic fingerprints) could be utilized to mitigate repudiation risks.

3. *Security Protocols and Prevention of Unauthorized Access and Modification*. An electronic signature process must prevent unauthorized access to the collection system used to affix electronic signatures to documents and records. The collection process must ensure that only authorized persons can access the system, prevent unauthorized signing or alteration of documents, and it should preserve a record of what modifications were made, by whom, and on what date/time. Additionally, internal electronic signature collection processes must prohibit individuals from affixing electronic signatures to records after the individual leaves the Department or terminates employment.

4. *Permanent and Unalterable*. Security protocols and records management functions must support the requirement for electronic signatures to be a permanent part of the record or document to which it was affixed, and the information contained in the record or document must be unalterable.

5. *Identification and Authentication*. When a higher level of non-repudiation is required, electronic signature collection software or other identity validation means should have identity verification and authentication capabilities that can identify a signature as belonging only to a particular person. The signer using the electronic signature should be required to use a method of identity verification and authentication (e.g., PIV card, biometric) that positively identifies the individual within the electronic signature system at the time of execution of the signature or the e-signer must be positively identified before affixing the electronic signature. Levels of authentication may depend upon the risk of repudiation for any given document or record. Components must consult with DHS OGC or Component Counsel(s) when determining what level of identity verification and authentication is appropriate to mitigate repudiation risks for particular documents and records.

6. *Corrections and Updates*. An electronic signature process should include a means for a signer to correct records or documents that were electronically signed in error prior to final submission of a document. The process should also allow for correction of documents that were properly electronically signed, but which contain information or data errors. When a record is corrected:

- The new information and new signature should be easily identifiable.
- The previous electronic signature and associated record should be voided.
- The information or signature being corrected should be retained as a new document or record (current version).

[3] As defined in Electronic Records and Signatures in Global and National Commerce Act, Pub. L. No. 106-229 (2000).

7. *Archivable*. The electronic signature process must have means of safely archiving electronically signed documents or records. The archiving process must produce, in a reasonable timeframe to support the need, a copy of each electronically signed record for transmission and storage in the appropriate IT system based on the document or record signed. For purposes of this requirement, any internal Agency document that is electronically signed must be electronically maintained by the Agency to protect the integrity of the electronic signature and document contents and must be stored in accordance with the applicable records schedule and security requirements. While this guidance does not require Components adopt any specific records management system or transmission approach, offices should work with their Component Chief Records Officer and CIO to satisfy this requirement.

5.0 PROCEDURES

1. Components shall integrate and standardize electronic signature collection processes as part of all document and records being electronically signed and Paperwork Reduction Act processes while leveraging investments in existing Agency records management systems or information technology investment. Electronic signature collection methods should be used whenever practical, except where handwritten signatures are required by law, regulation, Executive Order, or other requirements. Electronic signatures, including digital signatures, when properly executed, are to be accepted to the maximum extent practicable.

2. Electronically signed records must be maintained in accordance with operational and legal needs (including those of other federal agencies), perception of risks, and historical value, and retention should be formalized through corresponding Records Disposition Schedules approved by the National Archives and Records Administration (NARA). Operational and legal needs will ensure the availability, accessibility, and trustworthiness of electronically signed records over time and based on the need for the agency to comply with any court mandated orders or settlement agreements. Components should consult with their Chief Records Officer and Component Counsel(s) to clarify guidance and promote record retention requirements.

3. The visual context of an electronic signature (markings, graphic, or other identification of a signature) shall be maintained with the document or record for display purposes whether electronically or in hardcopy. DHS or other parties relying on the electronically signed document, transaction, or communication should be able to view the exact format and content of the document, transaction, or communication, that the signer reviewed prior to affixing his or her electronic signature to the record.

4. Where a DHS organization is relying on an electronic signature executed on a non-DHS system by an external signer using a digital signature or other acceptable electronic signature method, the DHS entity, in coordination with the DHS OGC or Component Counsel, determines whether the asserted signature is of an acceptable form and the signing date and time is sufficiently accurate and trustworthy to warrant acceptance for the intended use of the signature.

5. DHS OGC or Component Counsel, as appropriate, in coordination with Component CIOs and in consultation with relevant Component Forms Officials and the Component Chief Records Officer, will review and approve the adoption and integration of legally binding electronic signature capabilities into workflows and business processes for specific document types, forms, and other records, as needed.

6. Additional Component officials (e.g., CISO; Privacy Officer; Chief Financial Officer; Component CIOs) with equities in the electronic signature collection and retention process, should review and recommend adoption of electronic signature collection processes when appropriate.

7. Before Components devise new forms or revise existing forms to comport with this guidance, they must consult DHS OGC or Component Counsel to determine which non-repudiation safeguards and electronic signature formats should be utilized based on the legal requirements as well as feasibility as an operational and/or policy matter and the document being signed.

8. Where applicable or required, electronic signature collection processes should contain a means for the signer to indicate they are using a translator or translation services to understand the electronic signature block, as well as the parameters and content of the record being signed. Appropriate means of indicating a signer is using a translation service may include: a check box, affirmation statement and signature, or other appropriate means.

6.0 AUTHORITIES/REFERENCES

Office of Management and Budget Documents

Circular A-130, “Managing Information as a Strategic Resource”

Memorandum M-00-10, “Implementation of the Government Paperwork Elimination Act” (OMB M-00-10)

United States Code

Government Paperwork Elimination Act (GPEA), Pub. L. No. 105-277 (codified at 44 U.S.C. § 3504)].

Electronic Records and Signatures in Global and National Commerce Act (E-SIGN), [Pub. L. 106-229, § 1, June 30, 2000, 114 Stat. 464, codified at 15 U.S.C. §§ 7001 -- 7006).

Uniform Electronic Transactions Act (UETA), approved by the National Conference of Commissioners on Uniform State Laws (NCCUSL) on July 23, 1999, adopted by 47 states as of November 2010.

E-Government Act of 2002, Public Law 107–347, 116 Stat. 2899, 44 U.S.C. § 101.

Federal Records Act (FRA) (44 U.S.C. § 3301).

Privacy Act of 1974, As Amended. 5 U.S.C. § 552a, Public Law 93-579, Washington, DC, July 14, 1987

DHS Policy

DHS Sensitive Systems Policy Directive 4300A

DHS Electronic Signature Policy Guidance, Oct. 2, 2015

7.0 DEFINITIONS

Electronic Signature - E-SIGN[4] defines an electronic signature as “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record.”

Internal – Internal to DHS or through a DHS system or process.

Identification Information – the specific data captured to identify the specific signer. This data provides a positive determination that the signature belongs to and was executed by the signee. This is based on the electronic signature type used. Examples could include the date, time, location, and IP address at the time of signing, a virtual fingerprint that is unique to a person or entity, or other forms of data.

External – A party outside of DHS or outside of a DHS process or IT system.

Non-repudiation - Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

Person - An individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.

[4] Pub. L. No. 106-229 (2000)

Appendix A: Determining Which Electronic Signature Method to Use - Risk Assessment and Cost-Benefit Analysis

When implementing electronic signatures for a specific use, or when determining what methods of electronic signatures should be accepted from an external party for a specific use, the following risk assessment and cost-benefit analysis process should be used to determine which electronic signature methods are acceptable, unless the Signers can use a PIV Card, DoD-issued CAC Card, PIV-I Card, or software-based Digital Signature certificate meeting the requirements specified in the DHS Electronic Signature Policy Guidance document, version 1.01, Section III. Policy Statement DS.1.

1. Risk Assessment

1) Evaluating the Likelihood of Successful Challenge to Signature

a) Parties to the Transaction

i) An intra-agency transaction

ii) An inter-agency transaction

iii) A transaction between a federal organization and a non-federal organization (state, or local)

iv) A transaction between a federal organization and a private organization – e.g., business, non-profit, association, etc.

v) A transaction between a federal organization and an individual

vi) A transaction between a federal organization and a foreign government.

b) Nature of the Relationship and Frequency of Transactions

i) An ongoing relationship between the parties

ii) A new relationship with a known party

iii) A new relationship with an unknown party

iv) One-time, occasional, or frequently reoccurring transactions

v) An in-person signing or a remote signing

c) Value or Significance of the Transaction

i) Transactions involving the transfer of funds

ii) Transactions where the parties commit to actions or contracts that may give rise to financial or legal liability

iii) Transactions involving information protected under state or federal law (e.g., privacy, national security, otherwise sensitive, etc.) – i.e., importance and value of the information involved

iv) Transactions where the party is fulfilling a legal responsibility which, if not performed, creates a legal liability (criminal or civil)

v) Transactions where the party is certifying information or statements which, if not true or accurate, creates a legal liability (criminal or civil)

vi) Transactions involving information protected under state or federal law (e.g., privacy, national security, otherwise sensitive, etc.) – i.e., importance and value of the information involved

vii) Transactions where the party is fulfilling a legal responsibility which, if not performed, creates a legal liability (criminal or civil)

viii) Transactions where the party is certifying information or statements which, if not true or accurate, creates a legal liability (criminal or civil)

d) Risk of Unauthorized Alteration or Other Compromise

i) Regular or periodic transactions between parties are at a higher risk than intermittent transactions because of their predictability

ii) The value of the information to outside parties

iii) Certain federal organizations, because of their perceived image or mission, may be more likely to be attacked independent of the information or transaction

2) Evaluating Extent of Resulting Loss or Adverse Impact

a) Whether Lack of Signature Invalidates Transaction

b) Whether Lack of Valid Signature Process Creates Vulnerability for Exploitation of System

c) Damages and Other Non-Monetary Impact

d) Need for Provable Electronically Signed Records at a Future Time

i) Transaction information may later be subject to audit or compliance.

ii) Transaction information will be used for research, program evaluation, or other statistical analyses.

iii) Transaction information may later be subject to dispute by one of the parties (or alleged parties) to the transaction, or by a non-party to the transaction

iv) Transaction information may later be needed as proof in court or another forum

v) Transaction information will be archived later as long-term or permanently valuable records

3) Determining the Overall Level of Risk

Categorize the likelihood of a successful challenge to the enforceability of the signature and the cost or impact of an unenforceable signature into "Low," "Moderate" or "High" categories. The overall level of risk can be determined by combining those determinations into a risk level matrix to make an overall risk determination of "Low," "Moderate" or "High" (essentially by multiplying the likelihood of a threat event succeeding by the cost or impact of an unenforceable signature), as illustrated in the following Table.

Likelihood of Threat Event Succeeding

Impact of Unenforceable Signature	**Low Likelihood**	**Moderate Likelihood (2)**	**High Likelihood**
Low Impact	Low Risk	Low Risk	Moderate Risk
Moderate Impact	Low Risk	Moderate Risk	High Risk
High Impact	Moderate Risk	High Risk	High Risk

2. Cost Benefit Analysis

Designing an appropriate signing process within the options available for the applicable Risk Level requires a cost-benefit analysis to address practical considerations and cost considerations.

1) Cost-benefit factors that should be considered for a given risk level include the following.

a) Technology Issues

i) Technology requirements of the electronic form of signature, including hardware and software requirements

ii) Technology requirements of the transaction, which may be driven by factors such as whether the transaction will involve remote or in-person signing, single or multiple signers, and one or multiple signatures by the same signer

iii) Technology available to the signing parties, including the hardware and software available to the parties, the range of authentication procedures available to the parties, and the communication capabilities available to the parties

iv) Availability of alternative electronic forms of signature, alternative methods of identification and authentication, and alternative methods of ensuring integrity of the signed record

v) Susceptibility of each potential electronic form of signature or technology to forgery, compromise, and/or repudiation

b) Requirements of the Signing Process

i) Portability of the signature process (i.e., is there a need for signing to occur in many different, and changing, places?)

ii) Suitability of the signature process for multiple signers on same record

iii) Suitability of the signature process for in-person transactions and for remote transactions

c) Capabilities of the Signing Party

i) Sophisticated or unsophisticated regarding the transaction

ii) Knowledgeable or not regarding the technology used for signing

iii) Access to needed technology or not

d) Cost of Implementing/Using the Signing Process

i) To the federal organization

ii) To the signer