U.S. Nuclear Regulatory Commission

Office of the Chief Information Officer

Identity, Credential, and Access Management
User Guides
Electronic Signature
Implementation Assessment Guide

Version: 1.1
Release Date: 09 29 2017

J. David Sulser
Christian Palmhede
OEDO Electronic Signature BPI Team

Revision History

Date	Version	Description	Author
08 25 2016	0.1	Management Directive content development	OEDO Electronic Signature Business Process Improvement (BPI) Team
10 19 2016	0.2	Content conversion to Web guidance	Christian Palmhede
02 21 2017	1.0	Initial release for MD review process	David Sulser
09 29 2017	1.1	Incorporate office comments, add ML references	David Sulser

SUNSI Review

Date	Version	SUNSI Item Codes	Review Finding	Reviewer
09 29 2017	1.1	Publicly Available	The Identity, Credential, and Access Management (ICAM) Electronic Signature Implementation Assessment Guide is designated as publicly available because the document does not contain allegation, investigative, security-related, proprietary, or personally identifiable information, or other sensitive NRC information. This designation does not need any markings on the document.	David Sulser

Signature Page

Content approved by

Digital Signature

J. David Sulser

Digitally signed by J. David Sulser
DN: c=US, o=U.S. Government, ou=U.S. Nuclear Regulatory Commission, ou=NRC-PIV, cn=J. David Sulser, 0.9.2342.19200300.100.1.1=200000619
Date: 2017.09.29 18:00:55 -04'00'

Table of Contents

Table of Tables

Table of Figures

1 Purpose

This Web guidance document (guide) assists U.S. Nuclear Regulatory Commission (NRC) staff in understanding and implementing electronic signature. In doing so, it promotes continued compliance with the Government Paperwork Elimination Act (GPEA) and associated Office of Management and Budget (OMB) guidance in NRC's dealings with external parties, and increases the efficiency of the NRC's own internal processes by promoting and facilitating use of electronic signature solutions that the agency already supports.

This guide focuses on the factors that may need to be considered when establishing or modifying a signing process for a given type of transaction or class of transactions. For instance, there might be a signing process for NRC employees concurring on documents, a signing process for signing NRC forms, or a signing process a licensee proposes to use for its own records to satisfy NRC recordkeeping requirements.

A signing process often supports a larger business process, such as a contract award or regulatory action. The Web guidance addresses only the signing process, not other aspects of a business process.

This guide should be referenced when establishing or modifying a signing process. Once a signing process has been established, individual signers simply execute the established process. For example, the signer may click on a signature box in a document and when prompted, insert his Federal standard Personal Identity Verification (PIV) card, and enter his associated personal identification number (PIN).

For tasks involving signatures applied by NRC personnel, this guide encourages use of government-issued PIV cards. In many cases, a digital signature using a government-issued PIV card is the simplest solution. The guidance provides specific instructions on implementing digital signature across a wide range of agency business processes. The guidance also recognizes that there are cases where it is appropriate to use other kinds of electronic signature that do not require a PIV card.

Because staff may at times need to consider or evaluate the adequacy of new and different electronic signature processes, this guidance describes the basic, generic framework that can be used to assess any signature process. Specifically, it describes how to:

1. evaluate the risks of using and accepting electronic signatures;
2. examine available electronic signature options;
3. ensure recordkeeping obligations will be met; and
4. enable compliance with applicable legal requirements.

Among other sources, this guide relies on the Federal Chief Information Officer (CIO) Council document, "Use of Electronic Signatures in Federal Organization Transactions," Version 1.0, dated January 25, 2013. In this NRC document, **bulleted lists** are used for arbitrary quantities and items of equal weight, and **numbered lists** are used for specific quantities and sequential steps. Punctuation in lists conforms to the structure and meaning of the text.

2 The Need for Electronic Signature Use and Acceptance

GPEA says the agency, in its dealings with external parties, must facilitate the use and acceptance of electronic signatures wherever practicable. GPEA also says electronic signatures must not be denied legal effect, validity, or enforceability merely because they are electronic. Thus, GPEA directed the OMB to develop guidance for agencies to use in implementing electronic signatures.

Accordingly, when interacting with the public and regulated entities in matters that involve a signature, the NRC is obligated to provide the option of using electronic signatures, and should do so in accordance with the GPEA guidance, unless providing the option of electronic signature is not practical.

Given current technological capabilities, the option of using electronic signatures should generally be practical. Further, where NRC personnel are responsible for applying signatures, providing for the use of electronic signatures instead of handwritten signatures is expected to reduce costs and improve efficiency, particularly when using technology the agency already supports and employees already regularly use (for example, PIV card technology).

3 Overview of Process for Implementing Electronic Signature

Creating a new signing process, modifying an existing electronic signing process, transitioning from a handwritten signing process to an electronic signing process, or determining the acceptability for NRC purposes of an electronic signing process that an external party proposes to use may be very simple to accomplish, or may involve several steps, depending on the circumstances.

For many signing processes involving signatures applied by NRC personnel, converting to electronic signature using government-issued PIV cards to generate digital signatures is a simple, straightforward process. This is because PIV card technology and equipment are already available to all NRC personnel, and a properly implemented digital signature process using a government-issued PIV card is already understood to be acceptable for all types of transactions, regardless of the transaction's risk level.

Additional user guides outline the steps to implement digital signature processes based on PIV cards for use by NRC personnel in the context of commonly used NRC software applications. Following the guidance in implementing a digital signature processes based on PIV cards for signatures to be applied by NRC personnel ensures that any applicable requirements of law, OMB guidance, and the electronic signature management directive are met. However, in some cases a more involved assessment may be necessary to ensure the signing process is appropriate for the intended purpose, such as:

- a signature solution based on PIV cards that is not already addressed in the guidance;
- an electronic signature process that does not use a PIV card; or
- a signing process that involves electronic signatures applied by external parties.

For those NRC signing processes that require a more involved assessment, the seven steps are:

1. Evaluate the risk of electronic signature in the context of the business process.
2. Select one or more suitable technology solutions.
3. Develop or adopt an intent to sign statement.
4. Identify what supporting records will be kept to validate the signature.
5. Specify how record integrity will be protected.
6. Ensure that agency recordkeeping obligations will be met.
7. Confirm that the Office of the General Counsel (OGC) has no legal objection to the proposed signature solution.

Guidance for electronic signature implementation is provided in four parts:

1. risk analysis
2. technology selection
3. recordkeeping review
4. legal review

Together, these four parts form a complete signature assessment. Conducting the risk analysis, and other parts of the assessment, is intended to save time and ease the burden on the owner of the signing process by providing decision support at each step.

Figure 1 illustrates the four-part process, recognizing that where the signature-related risks associated with the transaction type are obviously low, a formal assessment process is not required. Figure 1 also captures management's intent to digitally sign correspondence and standard PDF forms. The abbreviation "e-sign" refers to electronic signature.

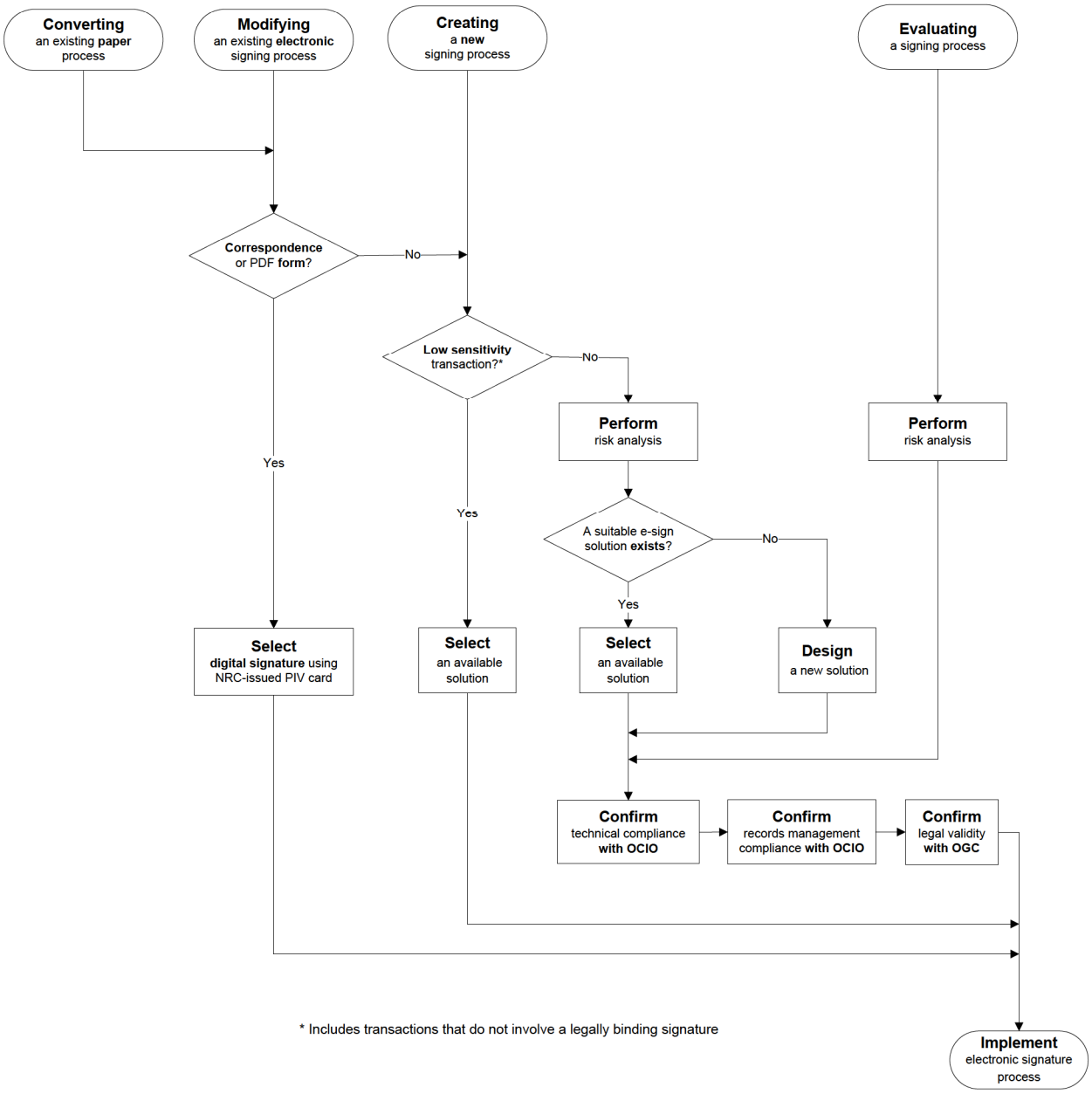

Figure 1: Process for Implementing an Electronic Signature

Later sections of this guide describe each step of the electronic signature assessment process in more detail.

The full signature assessment is focused on signatures made with the intent to bind the signer to the transaction—also called legally binding signatures—that are part of a signing process under the control of the NRC. There can be other implementations of electronic forms of signature not legally binding, such as signing e-mail to identify the sender. These are treated as low-sensitivity transactions and do not require a risk analysis. In such cases, you may find parts of the assessment useful to ensure technology compatibility, and if agency records are created, to meet recordkeeping obligations.

This guidance also applies to evaluating a signing process offered by an external organization to satisfy an NRC requirement. The signing process is often already in use outside the agency. Similar assessment activities are used to analyze risk and technology, as well as how agency recordkeeping and legal requirements can be met. The Office of the Chief Information Officer (OCIO) and OGC are available for consultation on evaluating external signing processes.

4 Determining Whether to Perform Signature Assessment

GPEA directed the OMB to "develop procedures for the use and acceptance of electronic signatures." These procedures are contained in OMB Memorandum 00-10, "Implementation of the Government Paperwork Elimination Act" (OMB M-00-10). The memorandum states:

> *GPEA recognizes that building and deploying electronic systems to complement and replace paper-based systems should be consistent with the need to ensure that investments in information technology are economically prudent to accomplish the agency's mission, protect privacy, and ensure the security of the data.*

To accomplish this, the OMB directs agencies to "develop and implement plans, supported by an assessment" that "should weigh costs and benefits and involve an appropriate risk analysis, recognizing that low-risk information processes may need only minimal consideration, while high-risk processes may need extensive analysis."

As indicated above, the user guides explain how to implement a signing process at the NRC involving digital signatures created using PIV cards in the context of commonly used software applications. When properly implemented, digital signatures using PIV cards can be used for even high-risk transactions. Further, the PIV card infrastructure is already in place, and PIV card use is already ubiquitous at the agency. Accordingly, a cost-benefit analysis would generally be unnecessary, as the agency has already incurred the most significant costs associated with NRC personnel use of PIV cards.

Other approaches to implementing electronic signature, however, may require you to perform a signature assessment to ensure the signing process is acceptable. Use your knowledge of the sensitivity of the underlying transaction to determine the need for a signature assessment. This document provides guidance on risk factors that may need consideration. Generally, low-sensitivity business processes and signatures that are analyzed as having low risk do not require a full signature assessment. For the purposes of this guidance, a low-sensitivity transaction is one where an erroneous or forged signature would have a negligible impact. Where the risk is low, you have broad discretion when using this guidance to implement electronic signature.

The need to weigh costs and benefits may depend on the extent to which a proposed signing process would use existing agency resources, systems, and processes. The NRC has already incurred acquisition costs and has justified ongoing expenditures for:

1. computer access for every staff member who needs it;
2. PIV cards for employees and contractors;
3. applications that can capture electronic signatures; and
4. IT infrastructure, both hardware and software.

Weighing technology costs and benefits is required only when a new signature technology is considered or a decision not to use electronic signature is proposed. In some cases, the added cost to external signing parties may need consideration. The remaining costs are (1) to develop specifications for how the staff will use these tools to apply signatures and (2) to train the staff so they can implement the process.

The purpose of an electronic signature assessment is to ensure that any risks associated with converting from paper to electronic or relying on electronic processes are properly identified and mitigated.

To streamline the evaluation, this Web guidance is narrowly focused on:

- determining risk;
- selecting a technology solution;
- ensuring intent to sign;
- demonstrating signature validity; and
- protecting transaction integrity.

The objective is to ensure that low-risk transactions can be rapidly assessed, while higher risk transactions receive the attention needed. For low-sensitivity transactions, you decide which parts of the assessment, if any, are needed.

Similar types of transactions can be treated as a single assessment. In other cases, analysis of a similar transaction can be reused. Grouping similar types of documents or transactions for the purpose of a signature assessment is encouraged.

A signature assessment is not needed when electronic signature is used only for personal identification, such as routine signing of e-mails, or signing personal documents, including when signed using a PIV card.

In cases where the use of signature does not convey any intent to bind, the risk analysis portion of the signature assessment is not needed.

All staff are encouraged to assess the potential for moving from paper-based transactions with a handwritten signature to electronic transactions with an electronic signature. This conversion may reduce cost or risk even though the underlying business process is unchanged.

Selecting a signature technology and signing process supported by the agency simplifies the assessment. This is especially true for digital signatures made using a PIV card. User guides provide specific information on using signature technologies already supported by the agency, and are the primary resource for you as you implement these technologies.

5 Preparing for Electronic Signature Assessment

For signing processes that would not simply involve NRC personnel digitally signing documents in commonly used software applications, a signature assessment may be necessary to ensure adoption of an appropriate signing process.

Many considerations go into a decision to use or accept electronic signature. These include business benefit and risk, technology choices, recordkeeping responsibilities, and legal

sufficiency. The considerations listed below help prepare for a streamlined signature assessment:

- who is signing
- how many are signing
- what each signature means
- relations among the parties
- potential value of the signed transaction
- frequency of signing transactions
- proximity of signing parties
- portability of signing process
- financial and legal liability

Practicality of signature technologies

- access to signature technologies
- familiarity with signature technologies
- cost of both implementing and using signing processes
- cost to the signers
- cost to the agency

Compliance considerations

- audit and regulatory compliance
- privacy and confidentiality

Challenges to signed transactions

- repudiated signatures (“I didn’t sign it”)
- denial of intent to sign (“I didn’t understand that I was signing”)
- contested integrity (“It’s my signature, but this is not what I signed”)

Record keeping needs

- reliability and preservation of the signed record
- protection of integrity
- maintenance of supporting records

You should consider any other risks relevant to your particular process. When preparing for a signature assessment, you should recognize that the assessment can mitigate identified risks and issues to acceptable levels through informed decision-making and planning. The guidance can be used when selecting technology solutions at different risk levels, and help guide the risk mitigation. When you choose an existing signature technology, the guidance describes how to meet associated technical, recordkeeping, and legal requirements.

The result should be a signing process that is useful, trustworthy, and appropriate for the risk level determined by the signature assessment.

6 Signature Assessment

Any process of expressing acceptance, acknowledgment, agreement, approval, authorization, certification, or concurrence in a manner that is intended to be binding is a signing process. OCIO has established electronic signature solutions that are available for agency use; office directors and regional administrators select which electronic signature solution to use for signing processes within their respective areas of responsibility. While the Web guidance describes digital signature solutions based on PIV cards that can be readily implemented for signatures to be applied by NRC personnel, and for which the assessment discussed in this document would not be necessary, other types of signing processes may require a signature assessment.

For nearly all signed transactions, a handwritten signature is less efficient than an electronic one. Thus, the agency's policy is to use electronic signatures whenever practical. You are also encouraged to assess the benefit of moving from a paper-based transaction (with a handwritten signature) to an electronic transaction (with an electronic signature), even when the business process itself is unchanged. A signature assessment may be important if significant features change regarding a transaction type that already uses electronic signature. For instance, if the nature of the parties to the transaction changes, if the effect of the signature changes, or if the value of the transaction type will be greater than before, a signature assessment would be important to confirm that the existing electronic signing process remains adequate. Signature assessments may also assist you in determining which particular electronic signature solution would be best suited to the task at hand.

6.1 Risk Analysis

Understanding the risks associated with a transaction means understanding:

1. the likelihood that someone will challenge the signature; and
2. the impact of a successful challenge.

Identifying the likelihood and impact yields an overall risk level. This overall risk level supports your technology selection and legal review.

When exploring whether a signing process is reliable enough for the sensitivity of the transaction, you need at a minimum to consider:

- the nature of the relations among the parties;
- the value of the transaction;
- the risk of unauthorized change; and
- the likely future need for available and credible information about the transaction.

You should also consider any other risks relevant to your particular process. Once you have considered these factors separately, you should consider them together to evaluate the overall risk, compared with the benefit the process brings. Lastly, when evaluating risks, you should consult with legal counsel about legal implications.

Once you have made that evaluation, you can select, or design if necessary, a technology solution that considers the risk level determined by the risk analysis as well as practicality.

6.1.1 Likelihood of a Challenge to Signature Validity

Analysis of the likelihood of a challenge considers how likely it is that a signer or a third party might challenge the signature. For instance, a challenger may deny that the signer meant to sign (intent to sign) or assert that the record is not what was signed (integrity of the record). You use your knowledge, experience, and good judgment for this likelihood analysis.

The points that you should consider when looking at likelihood are:

- the parties to the transaction;
- the relationships among the parties;
- the frequency of interactions among the parties;
- the proximity of the parties when signing;
- the importance or value of the transaction;
- the potential that the transaction could be compromised; and
- the potential for future examination of the transaction.

This analysis uses values of *low*, *moderate*, or *high* to represent the likelihood of a successful challenge to the validity or enforceability of a signature.

Who are the parties to the transaction?

One important consideration in evaluating the risk that a signer will challenge an electronic signature is the nature of the parties involved. For instance, the risk of a challenge is greatest with consumers, less with businesses (especially larger businesses), still less with state and local government, and even less with other Federal organizations.

What are the relationships among the parties?

Lasting relationships carry lower risk. Transactions between the agency and a publicly traded corporation or other known regulated party normally bear a low risk of challenge to a signature. This is especially true where the regulatory agency has enforcement authority over the entity. OMB notes that, “risks tend to be relatively low within rulemaking contexts, as all parties can view the submissions of others so the risk of imposture is minimized” (OMB M-00-10). Transactions with nonfederal parties where the agency has a law enforcement duty, but does not have a continuing relationship, carry higher risk.

Transactions between the agency and a foreign entity may entail unique legal risks because of varying national laws and regulations.

What is the frequency of interaction among the parties?

Risks are lower in cases where the parties engage in frequent transactions. The highest risk of fraud or challenge is for a one-time transaction between the agency and an individual that has legal or financial implications.

What is the proximity of the parties when signing?

You should consider whether the parties sign transactions face-to-face. Remote signing is often desirable but may call for additional mitigation of risk.

What is the importance or value of the signed transaction?

The more valuable a transaction, the greater likelihood a party will challenge it. While the government often measures value in dollars, other measures are also relevant, such as regulatory outcomes. Examples of low-risk transactions include where no funds are transferred, no financial or legal liability is involved, and no privacy or confidentiality issues arise.

Note the value of the transaction depends on the perspective of all involved parties, not only yours.

What is the potential that the transaction could be compromised?

The chance of a breach of the signed transaction increases the likelihood of a challenge, especially if the breach may affect integrity. Further, the chance of a breach increases with the potential benefit to the attackers and their knowledge of the transaction. Regularly scheduled transactions carry a higher risk. The purpose of an attack may only be to disrupt the transaction.

6.1.2 Impact of a Successful Challenge

Identifying the likelihood of successful challenges of a signature is the first part of the risk analysis. Next, you should consider the extent of any adverse consequences of a successful challenge (for example, regulatory, legal, and financial impacts). This is a comparison between the value of the signed record and its value without a signature.

As with the likelihood analysis, the analysis of the cost or impact of an unenforceable signature results in a determination that it is *low*, *moderate*, or *high*.

The effect of an invalid signature on the enforceability of the transaction

For transactions where law mandates a signature, a successful challenge to the signature usually annuls the entire transaction. For transactions not required by law to involve a signature, a signature may nonetheless provide useful evidence of a party's intent, but a successful challenge to the signature would eliminate that benefit.

The monetary and non-monetary value of the transaction

Where the lack of an enforceable signature annuls the entire transaction or makes proving its validity more difficult, you should consider the value of the transaction. For many transactions, the dollar value of an annulled transaction may not be easily calculated, yet the loss may be substantial due to the non-monetary value.

The durability of the signature

Some transactions need to be proved long after they are approved. Examples include where transaction information may be subject to audit or compliance, used for research or statistical analyses, subject to dispute or court challenge, or when transaction information becomes a valuable permanent record.

6.1.3 Determining Overall Risk Level

The analysis of the likelihood of a successful challenge and the impact of an unenforceable signature each result in a low, moderate, or high determination. You should then combine those results to get an overall signature risk level for the signed transaction of *low*, *moderate*, or *high*, as shown in Table 1.

Table 1: Determining Risk Level

	Low Likelihood	Moderate Likelihood	High Likelihood
Low Impact	Low-Risk Transaction	Low-Risk Transaction	Moderate-Risk Transaction
Moderate Impact	Low-Risk Transaction	Moderate-Risk Transaction	High-Risk Transaction
High Impact	Moderate-Risk Transaction	High-Risk Transaction	High-Risk Transaction

You should use the overall risk level to select technology solutions, and later, to evaluate associated legal and records management considerations. Supplemental Web guidance lists several technology solutions that are available from and supported by OCIO.

6.1.4 Electronic Signature Assessment Form

An assessment form in Microsoft Word format that can be used as an aid in the assessment will be developed and maintained as part of the Web guidance library. The form facilitates collection and evaluation of the information described in this section.

6.2 Examining Available Technology Solutions

You have discretion when selecting technology solutions for signing records. However, you rarely need to develop a signature technology solution. Supplemental Web guidance lists existing technology solutions for high-, moderate-, and low-risk implementations. For transactions where all signers have a government-issued PIV card, the NRC recommends using digital signature.

A technology analysis can aid you in finding the solutions that fit your defined risk level. This analysis addresses the practical considerations that may compel or rule out alternatives for signatures. If none of the available technology solutions adequately addresses the needs, you may need to evaluate and test alternatives. OCIO is available to assist you with technology analysis.

Finally, supporting more than one technology solution for a particular transaction may meet the needs of a greater number of signers.

6.2.1 Signature Technology Analysis Form

The assessment form in Microsoft Word format that will be developed and maintained as part of the Web guidance library includes support for electronic signature technology analysis.

6.3 Identifying Supporting Records

The records needed to prove or support the trustworthiness of the signature are called trust records. Supplemental Web guidance identifies trust records that should be kept to provide trustworthiness. For each risk level, the guidance lists the records that must be kept for trustworthiness (required), what records significantly back it (strongly advised), what records notably back it (advised), and what records provide some backing (optional). You must justify the exclusion of any supporting records for which inclusion is strongly advised.

The risk level identified in the risk analysis guides the decision on what supporting records to keep. If a risk analysis has not been done, the requirements for high-risk transactions must be satisfied. The supplemental Web guidance includes tables identifying specific records that are used to support the trustworthiness of electronic signatures, together with the requirements for using supporting records. The following stipulations apply when identifying supporting trust records.

- The parties that rely on the signed transaction should hold the supporting records associated with the signature.
- The signing parties may have records associated with the signature. The guidance lists supporting records the signer may have to make available.
- The process owner holds supporting records associated with the establishment and maintenance of the signing process.

OCIO provides supporting trust records for digital signatures created using NRC-issued PIV cards. The guidance has information on what records OCIO makes available.

6.4 Protecting Record Integrity

To protect the integrity of signed transactions, they must be stored on systems with a commensurate level of integrity. For example, a moderate integrity system may be used to store records from low- and moderate-risk transactions, while a high integrity system is needed for records from high-risk transactions.

Table 2: Protecting Record Integrity

System Security Categorization	High-Risk Transactions	Moderate-Risk Transactions	Low-Risk Transactions
High Integrity Categorization	✓	✓	✓
Moderate Integrity Categorization		✓	✓
Low Integrity Categorization			✓

6.5 Addressing Recordkeeping Obligations

Electronically signed records, as well as all supporting trust records, must meet the requirements of management directive 3.53, “NRC Records and Document Management Program.” Supporting records have a retention schedule at least as long as the records they support. The agency must preserve supporting records that validate the signature at least as long as the signed records’ retention period.

For the particular form of signature used, for example clicking on an “I Agree” button, the system must record and retain the records that validate that form of signature for the duration of the retention period.

Records related to the signature that are created, received, and maintained as part of an electronic transaction must be stored and preserved for the retention period the agency defines.

6.6 Ensuring Future Validation of Signatures

You must ensure trust records associated with signatures and deemed essential in validating those signatures remain available to validate the signature for as long as necessary to meet the

identified legal and recordkeeping requirements. OCIO must, to the extent possible, ensure that the signature technology selected will remain usable for purposes of signature revalidation for the lifetime of the transaction.

6.7 Deciding Against Electronic Signature

This applies if you or your office director or regional administrator decide (with or without a signature assessment) not to update a business process that uses handwritten signatures to use electronic signatures.

> A decision to reject the option of electronic filing or record keeping should demonstrate, in the context of a particular application and upon considering relative costs, risks, and benefits given the level of sensitivity of the process, that there is no reasonably cost-effective combination of technologies and management controls that can be used to operate the transaction and sufficiently minimize the risk of significant harm (OMB M-00-10).

7 Considerations When Implementing a Signing Process

7.1 Legal Criteria

If the law requires a signature, it is critical that an electronic signature and the signing process satisfy all requirements for a legally valid and enforceable signature. Even where the law does not require a signature, if an office determines that a signature is desirable for a given type of transaction, satisfying the legal requirements for a signature helps ensure that the signature serves its intended purpose. Where a signature is not required by law, electronic signature is nevertheless recommended:

- if there is a need for emphasizing the seriousness of the transaction, or
- if there is a need to bind a party to a specific intent in the transaction.

For example, the latter condition can occur when the transaction involves an intent to agree, approve, acknowledge, receive, or witness by a party.

For technology solutions already made available by the agency and described in the supplemental Web guidance, the guidance identifies how each solution might be implemented to satisfy the requirements for a legally binding signature. You may use this information to assess the ability of different technology solutions to meet office requirements for a valid signature.

In the event OCIO plans to address a new or modified electronic signature solution to facilitate future use of that solution by the agency, OCIO will coordinate with OGC to ensure that the discussion of legal criteria in the supplemental guidance is consistent with the legal criteria outlined below.

When you are considering whether to use or accept a new or modified electronic signature solution not already addressed in the guidance, determining whether the proposed solution meets the necessary legal requirements requires collaboration among OCIO, OGC, and the offices responsible for the transactions involved.

The CIO Council guidance distilled five requirements from the applicable laws that must be satisfied to create a valid and enforceable electronic signature:

1. A person (that is, the signer) must use an acceptable electronic ***form of signature***;
2. The electronic form of signature must be executed or adopted by a person with the ***intent to sign*** the electronic record (for example, to indicate a person's approval of the information contained in the electronic record);
3. The electronic form of ***signature must be attached to or associated with the electronic record*** being signed;
4. There must be a means to ***identify and authenticate*** a particular person as ***the signer***; and
5. There must be a means to preserve the ***integrity of the signed record***.

As electronic signatures are functionally equivalent to handwritten signatures, these five requirements also apply to handwritten signatures. The five requirements together must be met in a way that ensures the electronic signature is as reliable as appropriate for the purpose of the transaction.

Satisfying the five signing requirements calls for a signing process that may involve multiple steps, processes, or procedures. In some cases, the electronic form of signature chosen (for example, digital signature) can satisfy the majority of the requirements. In other cases, additional security procedures are needed.

7.2 Developing an Intent to Sign Statement

Intent is the critical component of any legally binding signature. Merely applying a sound, symbol, or process that is commonly used as a form of signature does not make it a legally binding signature. The signer must do so with an intent to sign—that is, with an intent to perform a legally significant act. Intent to sign is different from the *reason for signing*, which must also be made clear in the signing process. A reason for signing might be to agree to the terms of a contract or to attest to statements in the record, and is typically contained in the content of the record.

To establish intent to sign, the signing process must provide clear and conspicuous notice to alert the signer that a signature is being created and that it will be legally binding. This notice should:

1. be provided before the act of signing;
2. include a description of the signing process;
3. include a clear statement of the reason for signing; and
4. include a statement that when the act is completed it will constitute the signer's legally binding signature.

In electronic transactions, providing adequate notice to the signer is often aided by introducing the act of signing with language like the examples in Table 3. Such introductory language is often followed by the reason for signing.

Table 3: Examples of *Intent to Sign* Clause

High-Risk Transactions	Moderate-Risk Transactions	Low-Risk Transactions
"By checking this box …"	"… by"	"Sign here"
"By clicking the 'Next' button …"	"Sign here"	"Signature"
"By clicking the 'Submit' button …"	"Signature"	
"By entering my initials …"		
"By providing your PIV card and entering your PIN number …"		
"By signing below …"		
"By typing my name …"		

The *reason for signing* is the specific purpose for signing the record. It might be specified in the text of the document being signed, explained in the text of an on-screen signing process (for example, in a pop-up box), or made evident through the structure of the signing process. Examples of this language are provided in Table 4.

Table 4: Examples of *Reason for Signing* Clause

High-Risk Transactions	Moderate-Risk Transactions	Low-Risk Transactions
"I agree to be bound to the terms of this contract"	"Acknowledged and agreed to"	[None]
"I attest to the party's signature"	"Accepted"	
"I authorize the tasks described in here"	"Authorized"	
"I certify the truth of this statements"	"Certified"	
"I concur with the arguments presented in here"	"Concurred to"	
"I confirm that I have read and reviewed this document"	"Validated"	
"I certify that I have had the opportunity to read and review this document"		

Using words like those in Table 4 also makes it clear that the signer, by signing, is undertaking a legally significant act. However, words like the language in Table 5 may be needed to indicate whether the signature will be *legally binding* as opposed to significant for other reasons.

Table 5: Examples of *Legally Binding* Clause

High-Risk Transactions	Moderate-Risk Transactions	Low-Risk Transactions
"Under penalty of perjury"	[None]	[None]
"This signature does not represent a legally binding commitment."		

Together with statements along the lines of the examples above, an electronic signing process can further strengthen the notice to the signer through techniques such as:

- asking a signer to confirm the signature after it has been applied.
- alerting the signer that a signature has been recognized and providing the signer the choice to cancel or continue.
- following the signature step with a submission step, specifying to the signer that the signed records are not effective until submitted.

In general, the more important and the riskier the transaction, the more valuable it is to incorporate techniques such as these into the signing process to bolster the notice provided to the signer. Even for low-risk transactions, the electronic signing process should ensure that signers understand which action constitutes a signature and what the reason is for applying it.

7.3 Multiple Signatures

When more than one signature is applied, you should clearly indicate the reason behind each signature. Importantly, if the reason for one signature is different from the reason for another (for example, if one person signs the document to concur on the document's content, while a second person countersigns to attest to the validity of the first signer's signature), this should be clearly indicated.

7.4 Anonymous Signers

There are cases where an electronic signature made using an anonymous credential may be desirable, for example, reporting nuclear safety allegations. These are special cases where the normal requirement to identify the signer is not met. However, not every use of electronic signature requires a legally binding signature. The agency recognizes that there are appropriate uses of anonymous credentials and anonymous signatures.

Appropriate use of anonymous electronic signature depends on the business process being served. In some cases, it may be sufficient to authenticate that the person is a member of a certain group or that he or she is the same person who previously supplied or created information. Furthermore, a person may be entitled to use a particular pseudonym. When using anonymous signature to protect privacy, the obligation remains to use the information collected only in a manner consistent with the reason for signing and with any assurances provided during the signing process.

8 Records Management Review

Offices using electronic signatures must comply with the applicable requirements in NRC Management Directive 3.53.

Records created, acquired, or retrieved that are related to a signature should be stored and preserved in accordance with the required retention periods identified in:

1. NUREG-0910, "NRC Comprehensive Records Disposition Schedule";
2. General Records Schedules of the National Archives and Records Administration; and
3. approved records retention schedules published on the agency's public website.

When you select a standard supported signature technology implementation, in particular a PIV card digital signature process as described in the guidance, the records management review

process is simplified. OCIO can advise on other implementations of electronic signature and will determine if the proposed design meets recordkeeping requirements.

9 Legal Review

Formal review by OGC is the last step in the process. When there is a proposal to use an electronic signature solution already supported by the agency and described in supplemental Web guidance, the guidance will identify what, if any, issues require an OGC review. But not all potential implementations of electronic signature will necessarily be addressed in the guidance.

This section addresses the general nature and purpose of an OGC legal review of an electronic signature process. It also provides guidance to you on facilitating OGC's review, which you should follow if specific guidance tailored to the signature technology you are considering is not available.

OGC's review assesses whether the proposed electronic signing process appropriately addresses any applicable legal risks and any other legal requirements or considerations. OGC's review would include, but is not necessarily limited to, analyzing whether the proposed signing process would satisfy the five basic legal criteria for valid, enforceable signatures in a manner that is as reliable as appropriate for the intended purpose. To facilitate OGC's review, you should be prepared to provide OGC with information on:

- what risks were identified in the risk analysis (if any);
- how the signing process identifies and authenticates the signer;
- how the signing process ensures that a signature is applied with an intent to sign;
- how the signing process identifies and communicates to the signer the reason for signing;
- how, and by whom, records regarding the various aspects of the signing process will be maintained;
- how the integrity of the signed records will be ensured; and
- whether the signing process involves personal information (that is, about the signer), and if applicable, what steps will be or have been taken to address any potential Privacy Act or other privacy-related issues.

Although OGC's formal review occurs at the end of the process, you are encouraged to consult with OGC before the formal OGC review stage if you identify any significant potential legal questions or concerns.

Consistent with the overall focus of this Web guidance on the signing process rather than individual signatures, this guidance does not provide for OGC review of individual signatures made under the terms of an approved signing process. Nevertheless, any actual or suspected legal issues that arise regarding electronic signatures—even individual uses of an already-approved signing process—may still be raised with OGC, as appropriate.

10 Training

For electronic signature technologies used by the entire agency, OCIO provides training guides and materials to assist you with the use and implementation of electronic signature. Guidance and training documents are located in the ICAM Electronic Signature folder in ADAMS. Open ADAMS Folder (Electronic Signature). The library currently includes the following guides:

- Electronic Signatures in Adobe Acrobat (ML16272A479)
- Electronic Signatures in Microsoft Word (ML16272A484)

For the office-specific signing processes they approve, office directors must provide training to the staff on the specific electronic signing process implementation.