Windsor Solutions



Submission Certification and CROMERR Overview

Updated For Version 4.9

Revision Date: July 27, 2020



THIS PAGE INTENTIONALLY LEFT BLANK

**Contents**

Submission Certification Overview 1

Registering a User Account 1

Understanding Authorization Types 1

Establishing User Authorization 2

Certifying a Submission 4

CROMERR Related Security Features 6

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Author** | **Date** | **Notes** |
| 3.3 | Windsor | 8/1/2014 | Initial version |
| 3.3 | Windsor | 8/17/2016 | Updated to include new ability to assign eSignatory and Verified user at the organization level.  Added additional CROMERR specific features. |
| 4.3 | Windsor Solutions | 12/19/2017 | Adjusted to reflect release 4.2/4.3. |
| 4.4 | Windsor Solutions | 1/10/2018 | Versioned for v4.4. |
| 4.4 | Windsor Solutions | 4/24/2018 | Added Guest Submission capabilities. |
| 4.5 | Windsor Solutions | 6/28/2018 | Updated to reflect release 4.5. |
| 4.6 | Windsor Solutions | 2/20/2019 | Updated to reflect release 4.6. |
| 4.6 | Windsor Solutions | 5/28/2019 | Updated to reflect new file system document storage option. |
| 4.7 | Windsor Solutions | 5/28/2019 | Versioned for 4.7. |
| 4.8 | Windsor Solutions | 1/29/2020 | Versioned for 4.8. |
| 4.9 | Windsor Solutions | 7/27/2020 | Updated to reflect 4.9. |

# Submission Certification Overview

nFORM is an electronic document receiving system that can be used by a regulatory agency to accept various types of applications and reports submitted by regulated entities and other external stakeholders. The system allows customers to register a single account that can be used to submit electronic documents to the agency.

Each type of document that may be submitted will require one of a number of levels of certification authority on the part of the submitting entity, ranging from simple registration to formal signature authority. Regardless of the required level of authority, nFORM will electronically certify and retain the submission. Additionally, where a formal signature authority is required, nFORM uses an electronic signature device to certify an electronic document submitted to the agency. The use of this electronic signature device establishes proof of identity and intent on the part of the submitting user, and is designed to be equivalent to a “wet ink” signature.

## Registering a User Account

nFORM allows users to create a user account via a registration process. During the registration process, the user provides information about themselves such as their name, phone number, physical address and a unique identifier, in the form of the user’s email address, to be used as the account login. No two users can have the identical user account logins, and account logins cannot be re-used if the original account login is no longer needed or used by a user.

When registering an account, the user will enter their desired system password. Passwords that do not meet the password format/strength requirements will be rejected, and the user will be prompted to re-enter a valid password. The minimum requirements within nFORM for password strength are:

* Must be at least 8 alpha-numeric characters
* Must include at least one upper case letter
* Must include at least one lower case letter
* Must include at least one numeric digit
* Must include at least one special character
* Must not have been used by the user previously

If the entered password adheres to the password requirements, the user’s password will be stored in encrypted format in the database and the user will be prompted to sign into the system. The system will also send a Password Reset email confirmation to the user.

nFORM will send an automated email to the user with a hyperlink used to confirm their email address. The user will need to click on the link to confirm their account in order to enable their user account. Until the user account is confirmed, the user will not be able to login to the account.

## Understanding Authorization Types

nFORM allows external users to have one of three types or levels of authorization:

1. **Guest Users** are those users who would like to submit a form in the NFORM system, without registering an account. This authorization level is enabled on a form-by-form basis, when appropriate.
2. **Self-Registered Users** are those for whom a user account and a profile exists in the nFORM system but who have not been further verified by program staff. For example, no confirmation has been conducted to determine if the account belongs to a “real” person.

This is a global security role, and applies to all organizations. The user with this role can complete and submit any (across all organizations) form marked with self-registered user authorization, unless the form is marked as Internal Only.

1. **Verified Users** are those whose user accounts have been verified by program staff by some means.

This is a scoped security role (by organization implicit or cascading), and applies to only the organizations to which the user has this role. The user with this role can complete and submit only those forms within their designated organizations for forms marked with verified user authorization, unless the form is marked as Internal Only.

1. **Electronic Signatory Users** are those users who have been further confirmed as having sufficient standing to have their electronic signatures considered as equivalent to paper signatures. This is usually done through a separate manual process involving confirming the user’s identity through a secondary means. (This method should be used for those forms that fall under CROMERR).

This is a scoped security role (by organization implicit or cascading), and applies to only the organizations to which the user has this role. The user with this role can complete, *sign* and submit only those forms within their designated organizations for forms marked with electronic signatory user authorization, unless the form is marked as Internal Only.

Each form in the nFORM system is configured to require one of the above levels of authority before submissions will be allowed from the user in question. The level of authorization required for each form will be determined at the discretion of the agency programs:

1. Forms that require only the self-registered level of authorization might be those expected from a wide and largely unknown universe of submitters.
2. The verified user level of authorization might be required for forms for which the submitter universe is relatively discrete and largely known.
3. Electronic signatory authority will typically be required if the regulatory requirement for the data collection specifies a signature requirement for hard copy submissions. Forms that fall under the requirements of the EPA CROMERR rule will require this level of authority.

## Establishing User Authorization

### Self-Registered Users

Upon initial user account creation in nFORM, all external users are given the self-registered level of authorization. This grants basic permissions to submit applications and reports that require no further verification of the user’s identity.

### Verified Users

Before granting the verified user level of authorization, agency staff will undertake steps to confirm that the user is an individual with a legitimate need to use the nFORM system to make electronic submissions to the agency in lieu of paper submissions. This process is essentially intended to eliminate user accounts that are automatically generated by Web tools, or by individuals with no valid reason to make submissions.

Steps that may be taken could include sending an email to the registered user to determine if the email account is monitored, or contacting the user by phone to inquire on the reason for their registration.

This role is applied at the organization level, and can be implicit (only the selected organization) or cascading (role applies to selected organization and all child organizations).

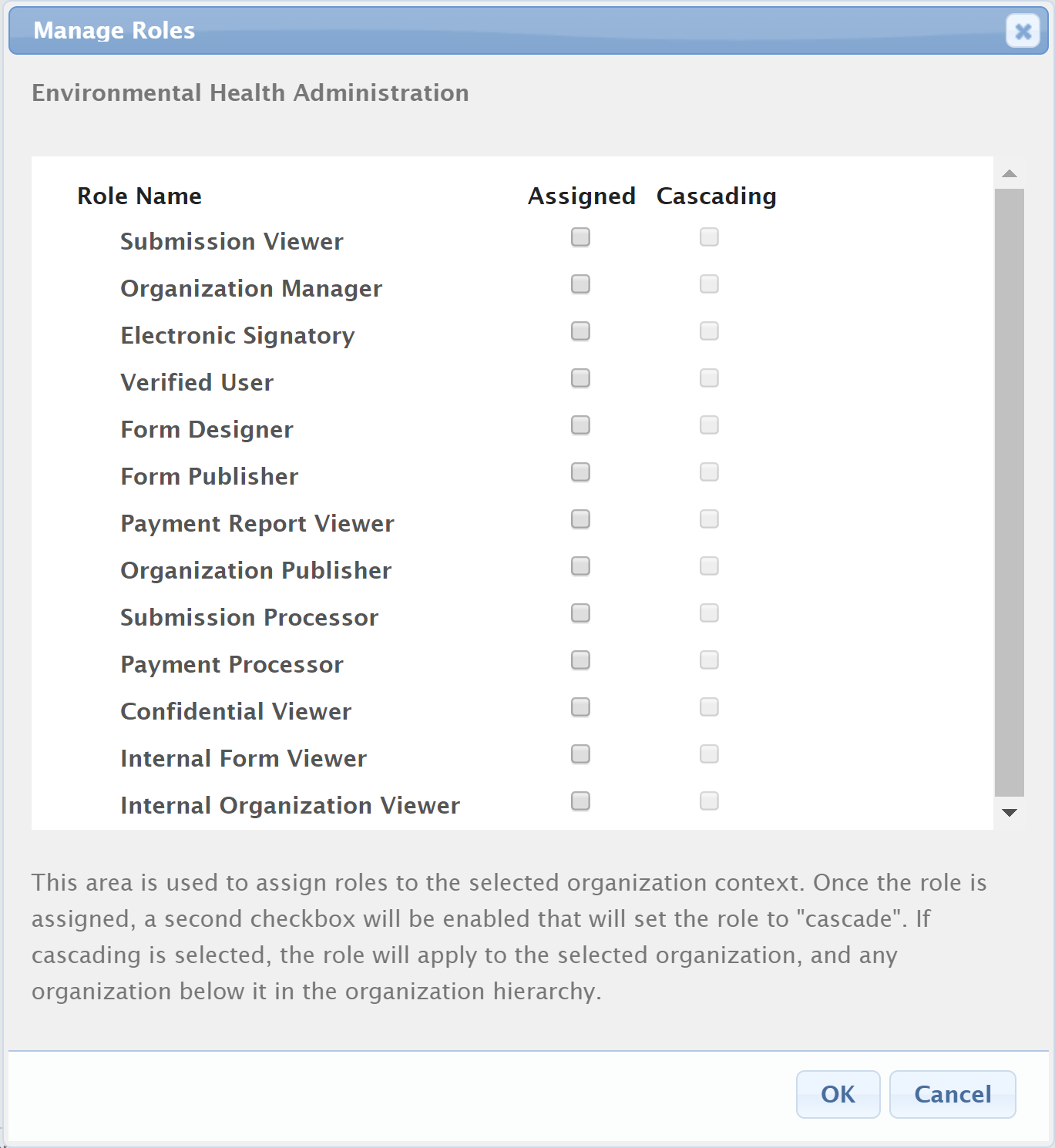


Diagram 1: Example of assigning the verified user to an Organization and its children (cascading)

### Electronic Signatory Users

Agency staff are able to grant the electronic signatory level of authorization to a user once that user has completed a further series of steps. These steps should allow the agency to positively confirm the user identity and meet the legal requirements to qualify the user’s future electronic submissions as equivalent to paper submissions.

In order to be further granted electronic signature permissions in nFORM, a user must first complete and submit a Electronic Signatory/Subscriber Agreement (ESA) to the agency. The ESA is a hardcopy electronic signature agreement signed by the individual with a handwritten signature which is mailed to the agency and manually reviewed. The form of the ESA may vary according to the specific needs of the agency but should require the information needed to provide sufficient proof of a user’s identity. The ESA should contain language requiring the user to protect their signing credentials, not to share signing credentials with anyone else, and immediately report any compromise of the credentials to the agency.

The agency will review the information provided in the ESA and perform additional identity proofing as needed. If needed, the agency has any questions about the persons identified, the individual is contacted and the information is verified. Once the ESA has been verified by the agency, the user will be granted electronic signatory authority within the nFORM system. This role is applied at the organization level, and can be implicit (only the selected organization) or cascading (role applies to selected organization and all child organizations). This will allow the user to submit applications and reports that require electronic signature authority for their organization(s).

Processed ESAs are typically retained in a secure location by the agency subject to the appropriate state or federal document retention policies.

Following a successful login to the system, if the agency has accepted and approved their ESA and the user has been granted electronic signatory authority, nFORM prompts the user to define their challenge questions and answers. The user is not forced to perform this step immediately; however, the system will not allow the user to submit a form which requires an electronic signature until this step is performed.

If the user does choose to setup their challenge questions and answers after their login, they will access their user profile, available as a hyperlink from within the application. The user is presented with 22 possible challenge questions, of which they are required to provide answers to 5 questions. Answers must be at least 5 characters in length and must be unique. A history of all challenge questions and answers used by the user account, along with their effective dates, is retained in the database. Once the challenge questions have been selected, answered, and successfully saved, the user is unable to view or change the questions and answers. They may contact the agency to have their challenge questions reset, which will “expire” all the current challenge questions and answers.

The user’s account identifier, challenge questions and answers together are used to establish the user’s electronic signature within the nFORM system.

## Certifying a Submission

### Self-Registered User and Verified User Forms

Forms that require the self-registered user level of authority may be submitted by any system users. Forms that require the verified user level of authority may only be submitted by users with either the verified or electronic signatory level of authority for their organization(s).

Once the user has completed the information required by the online form, nFORM will generate a read-only representation of the form submission and present it on the screen for the submitter to review before signing. The submitter must acknowledge that they have reviewed the form submission prior to completing the form submission process.

nFORM will then provide the user with a page displaying the agency-defined submission certification criteria that each submitter must agree to before they can proceed with the form submission process. By submitting the form, the user is acknowledging the certification agreements on the screen. The act of submitting the form therefore serves to certify the submission.

The unique user account login is then encrypted and is then bound to the submission which is also encrypted. The submission content and user account cannot be separated once accepted by the system and the combined artifact represents the formal “copy of record” for the submission.

### Electronic Signatory Forms

If a user has been granted electronic signatory authority and has established their challenge questions and answers, they may submit an application or report that requires an electronic signature.

Once the user has completed the information required by the online form, nFORM will generate a read-only representation of the form submission and present it on the screen for the submitter to review before signing. The submitter must acknowledge that they have reviewed the form submission prior to completing the form submission process. The PDF generated, and the files attached then are hashed to become immutable copies of record for the submission.

nFORM will then provide the user with a page displaying the agency-defined submission certification criteria that each submitter must agree to before they can proceed with the form submission process. By submitting the form, the user is acknowledging the certification agreements on the screen.

nFORM will also randomly choose one of the 5 challenge questions previously selected and answered by the user. The user must correctly enter the answer to the presented question. If a challenge question is incorrectly answered, nFORM will automatically cycle to the next challenge question. The act of providing the correct challenge question response and submitting the form therefore serves to certify the submission.

The unique user account login, challenge question and challenge question response is then encrypted and used as the user’s electronic signature to certify the submissions authenticity. This electronic signature is then bound to the submission which is also encrypted. The submission content and electronic signature cannot be separated once accepted by the system and the combined artifact represents the formal “copy of record” for the submission.

### Storing a Submission (Copy of Record)

As detailed above, nFORM will create a “copy of record” for each submitted form which will contain encrypted versions of the reported data, related attachments (if applicable), and identifying metadata, as well as either the encrypted user account or the encrypted electronic signature depending on the level of authorization required for the form.

nFORM will use a private certificate key provided by the agency to digitally sign the resulting copy of record and seal the document with the signatures intact. The copy of record will be in the form of a ZIP or PDF file, depending on whether attachments are included in the submission. If no attachments are included in the submission, the submitted form will include one PDF file representing the reported data. This PDF file will include the certificate. If attachments are included in the submission, the submitted form will include one ZIP file which will include one PDF file representing the reported data and all attachments included in the submission. This ZIP file will include the certificate.

Submitters are notified about the creation and storage of the copy of record in an automated email sent by nFORM. The user may access the electronically signed document at any time within nFORM. If the submitter needs to modify a submission, they must provide the revisions using an entirely new submission which can first be copied from the prior submission. The most recent form submission then becomes the user’s official copy of record but does not replace or delete any existing submission.

The user may also request that a submission be rescinded, for example, if submitted accidentally. Agency staff will review such requests and nFORM will notify the user accordingly.

The digitally signed, encrypted copy of record is stored in the relevant file storage system. There is no way within nFORM to modify a copy of record.

The integrity of the electronic certification and submission contents may be verified at any time by recalculating the signature and submission contents using the original encryption key. If any part of the copy of record was altered, including the electronic signature information, result would differ from the original, allowing the system to detect the change.

# CROMERR Related Security Features

It should be noted that a system alone cannot be deemed CROMERR compliant. Compliance is based on the systems specific implementation, both technical features and business process for each client’s specific usage. For example, if Arkansas DEQ submitted a CROMERR application for nFORM, and it was accepted by the EPA, then ARDEQ’s nFORM implementation can be considered CROMERR compliant. If New York DEC wished to obtain CROMERR compliance, they would need to submit an application for their implementation of nFORM.

Below are a list of feature in nFORM that are often included as necessary functionality in a CROMERR compliant system.

| **Requirement** | **Category** | **Subcategory** |
| --- | --- | --- |
| Allow users to create/register a new user account. This includes information such as name, phone number, physical address and unique login in the form of an email address. | User Management | Profile |
| User login must be unique | User Management | Login |
| User login cannot be reused | User Management | Login |
| The system must enforce a password strength with the following minimum parameters: - Must be at least 8 alpha-numeric characters - Must include at least one lower case letter - Must include at least one upper case letter - Must include at least one numeric digit - Must include at least one special character - Must not have been used by the user before. | User Management | Password |
| The system must provide the ability to automatically expire passwords. | User Management | Password |
| The system must maintain a history of all passwords used by the unique user account login in the database, including the date/time the password was created and expired. | User Management | Password |
| The system can only allow one active password for a unique user account login, at a given time. | User Management | Password |
| All user password must be stored in an encrypted format in the database. The format will be a one way, "salted", hash, using the SHA-512 bit algorithm. If needed, the algorithm can utilize the Bcrypt or SHA-3 algorithm, via configuration setting. | User Management | Password |
| After a user changes their password, the system will require that the user sign in to the system utilizing the new password. | User Management | Password |
| To overcome forgotten passwords, allow a user to enter their email address to request a change of their password. In order to initiate the password change process, one of their entered challenge questions will be randomly selected and will be presented. The user must answer the challenge question correctly to initiate the password change. If a challenge question is correctly answered, a new password is randomly generated by the system and emailed to the user's email address.  Note: For users who are not Electronic Signatories, they will not be required to enter a challenge question answer to request a password reset. | User Management | Password |
| After a user attempts to change their password, the system will send a Password Reset confirmation email to the user. | User Management | Password |
| The system must allow an Administrator or Organization Manager to reset a user's password, as required. When an Administrator or Organization Manager initiates the password reset, a new password is randomly generated by the system and emailed to the user's email address.  After a password is reset, the user will be required to change their password when attempting to login into the system for the first time before proceeding with system use. The user will be required to enter their current password as well as their new compliant password. | User Management | Password |
| The system must allow a user to change their password, if logged in. When attempting to change the password, the user will be required to enter their current password as well as their new compliant password. | User Management | Password |
| Upon registration of a new user, the system must send an email to the user with a hyperlink used to confirm their email address. | User Management | Confirmation |
| Allow a user to be assigned to the Electronic Signature role. | User Management | Role Assignment |
| Following a successful login to the system, if the user has Electronic Signature rights, the user must be prompted to define their challenge questions and answers. The user is not forced to perform this step immediately; however, the system will not allow the user to certify and submit a form (which requires an electronic signature) until this step is performed. | User Management | Challenge Questions |
| Once challenge questions are provided, the user will not have the ability to change the answers through their profile, unless their challenge questions have expired. | User Management | Challenge Questions |
| Allow electronic signatory users to establish challenge questions, if not established. | User Management | Challenge Questions |
| The system must enforce that challenge questions meet the following parameters: - Five challenge questions must be answered. - Each selected challenge question must be unique. - Answers must be at five characters in length or longer. - Answers must be unique across all five questions. | User Management | Challenge Questions |
| They system will allow users to select from a list of 22 challenge questions. | User Management | Challenge Questions |
| The date/time a challenge question answer was provided must be tracked. | User Management | Challenge Questions |
| A history of challenge questions and answers must be maintained in the database, including question, answer, effective dates and expiration date. | User Management | Challenge Questions |
| Challenge questions asked and the respective answers should be encrypted, per EPA recommendation. | User Management | Challenge Questions |
| The system must allow an administrator to expire a user’s challenge questions. | User Management | Challenge Questions |
| Challenge question answers must be stored in an encrypted format in the database. The format will be a one way, "salted", hash, using the SHA-512 bit algorithm. If needed, the algorithm can utilize the Bcrypt or SHA-3 algorithm, via configuration setting. | User Management | Challenge Questions |
| The system will automatically lock an account if the user attempts to change their password and incorrectly answers the challenge question on five (configurable) consecutive attempts. | User Management | Challenge Questions |
| All user session communication must be protected through SSL. | General | Communication |
| The Certify and Submit page consists of agency-defined electronic signature agreement criteria that each submitter must agree to before they can proceed with the form submission process. The user must individually acknowledge each agreement on the screen before they are allowed to continue. | Submission | Certification |
| Each agency must have the ability to customize their electronic signature agreement criteria to meet their requirements. | Submission | Certification |
| If all conditions (agreements) are accepted, the user must have the ability to electronically sign the submission, by a randomly selecting one of the five answered challenge question and entering their account password. If a user does not answer the selected challenge question correctly, the system will select the next challenge question, requiring the user to answer the challenge question presented and reentering their password. | Submission | Certification |
| The system must provide an automatic lockout mechanism based on a configurable maximum number of electronic signature (challenge question + password) attempts, with 5 being minimum setting. | Submission | Certification |
| At a minimum, the system must present the following agreements to the user signing the submission: - I am the owner of the account used to perform the electronic submission and signature. - I have the authority to submit the data on behalf of the facility I am representing. - I agree that providing the account credentials to sign the submission document constitutes an electronic signature equivalent to my written signature. - I have reviewed the electronic form being submitted in its entirety, and agree to the validity and accuracy of the information contained within it to the best of my knowledge.  Additional agreements can be added by the (Insert State/Agency System Acronym). | Submission | Certification |
| The system must allow a custom certification statement to presented to the user for CROMERR certifications. | Submission | Certification |
| The system must support a digital signature process utilizing X509-compatible certificates. At a minimum, it must support a PKCS#12 (PFK) type. | Submission | Signature |
| The system must support SSL communication (i.e., strong 256-bit encryption 2048-bit root) for the electronic signature process. Note that the electronic signature certificate is different from that used by the solution to secure its communication (which uses the SSL certificate). | Submission | Signature |
| During the form submission process, the system will generate a read- only representation of the form submission and present it on the screen for the Submitter can view the form submission before signing. The read-only representation of the form submission includes all data contained within the form submission as well as the ability to download and/or open any related attachments that the Submitter included in their submission. The Submitter must acknowledge that they have reviewed the form submission prior to completing the form submission process. | Submission | Submission |
| The certification statement presented to the signer, including warning of penalties for false certification, must be incorporated into the copy of record for the signed submission. | Submission | Submission |
| The system must protect the integrity of the form submission by, not allowing alterations of the form submission content during transmission or after it is received. | Submission | Submission |
| The system must protect the integrity of the form submission by, utilizing SSL for the entire form submission process, protecting the system and submission against man-in-the-middle attacks. | Submission | Submission |
| The system must protect the integrity of the form submission by, sending an email notification after each form submission. This email contains a unique submission number as well as a link to the submission record where the electronically signed CoR can be downloaded. | Submission | Submission |
| The information used to populate the read-only representation of the form submission, reviewed by the Submitter during a form submission, must be the exact information used to complete the form submission. No updates to that data previewed can be made after the submission process begins. | Submission | Submission |
| The CoR must contain the exact data used to populate the read-only view of the form submission, reviewed by the Submitter during a form submission. | Submission | Submission |
| The system must allow the unique user account login, password, challenge question and challenge question response to be used as the electronic signature device. The application must use its private certificate key to digitally sign the hash of the signature device and the CoR to bind the electronic signature to the submitted form. | Submission | Signature |
| The electronically signed CoR file created for each submitted form must contain the reported data, header page, related attachments (if applicable) and bound electronic signature. The electronically signed CoR file created for each submitted form will be in the form of a ZIP or PDF file, depending on whether attachments are included in the submission. If no attachments are included in the submission, the submitted form will include one PDF file representing the reported data. This PDF file will include the certificate. If attachments are included in the submission, the submitted form will include one ZIP file which will include one PDF file representing the reported data and all attachments included in the submission. This ZIP file will include the certificate. | Submission | Submission |
| The CoR must contains a header page with meta-data from the submission process, including date and time of submission, submission number and submitter name. A watermark indicating the certificate authority used and fingerprint (a unique certificate number) for the electronic signature is also displayed. No passwords, challenge questions/answers, or any other sensitive information is displayed on this header page. The header page is included in the CoR strictly as a clear way of visibly indicating to any viewer of the CoR that the CoR has been successfully electronically signed. The meta-data recorded on the header page is retrieved from the database, so it's not the sole source of this information. | Submission | Submission |
| Upon submission of an electronic signature level form, a copy of record of the submission at submission time, must be retained. | Submission | Submission |
| Following the submission/signature, the system must present the submitter with a confirmation page including a unique Submission Number. | Submission | Submission |
| The system must send an acknowledgement email to the email address of the Submitter after every submission. The email will contain the Submitter's name, date and time of submission, subject of email, as well as a unique Submission Number, so that the Submitter can further identify the form submission in question. This email contains the unique confirmation number and a description of where to download the CoR within the system, if desired. | Submission | Submission |
| Following the submission/signature, the system must provide the ability for the Submitters to view or download the electronically signed copy of the CoR at any time for any form submission (where they are assigned as a contributor to the form submission) from the Submission View page of the nFORM system. | Submission | Submission |
| The electronically signed version of the CoR must also be able to be used for verification of signature authenticity, and that no modification to the CoR has been made since initial creation. The system must be provide the ability to Verify Authenticity of a COR. | Submission | Submission |
| The system must store the CoR (i.e., PDF and associated attachments) as a two-way hash, using the SHA-2 512 bit algorithm. If needed, the algorithm can utilize the Bcrypt or SHA-3 algorithms, via confirmation setting. COR's are protected from deletion or alternation through hashing. | Submission | Submission |
| When providing the human readable CoR to a user for download and access, the CoR must first decrypted, using the decryption key. The decryption key must be stored in the application configuration file.  There can be no separate step required to make the CoR human readable, except that the browser or local user's computer must be capable of opening a ZIP files (if applicable) and rendering PDF documents as well as well as any applicable attachments provided by the Submitter. | Submission | Submission |
| The system must provide the ability to "Recind" a submission. | Submission | Submission |
| The system can provide no function to modify or delete a COR. CORs must be retained indefinitely. | Submission | Submission Management |
| The system must provide the ability to view all submissions and their status, including any form submissions that were rescinded. | Submission | Submission Management |
| The system must provide the ability to lock a user account. | User Management | Locking |
| The system must provide notification to a user, if their account status is changed (e.g., locked and unlocked). | User Management | Locking |
| The system must provide the ability to print the COR. | Submission | Submission |
| The CoR must be stored in the database in the Binary Large Objects (BLOB) format or on a relevant file system in an encrypted format. | Submission | Submission |
| The system must assign each CoR a unique document identifier that is related to the submission. | Submission | Submission |
| The system must provide the ability to log items in a database audit table as well as the application event logs. The individual entries in these two logs must be identical in information and format to allow comparison.  Each audit log will need to include the following information:  -- Submission Number (including revision number), if applicable -- What action was taken -- When the action took place -- Who performed the action (name and user id) -- User impacted (if different from user taking action). For example if an internal user initiates a password change for another user. -- Link to CoR -- Other pertinent details (e.g., what challenge question(s) was used, etc.) | User Management | Audit Logging |
| The system must log password change attempt to the audit logs, with a pass/fail indicator. | User Management | Audit Logging |
| The system must log challenge question change attempt to the audit logs, with a pass/fail indicator. | User Management | Audit Logging |
| The system must log electronic signature attempts to the audit logs, including success or fail indicator, and source of issue (challenge question response attempt) if failed attempt. This log will include the challenge question selected as well as the acknowledgements agreed upon. | User Management | Audit Logging |
| The system must log submission status changed (rescinded, revised, issued, etc.) to the audit logs. | Submission | Audit Logging |
| The system must log email notifications that are sent to the applicant to the audit logs. | Submission | Audit Logging |
| The system must log submission processing step status changed to the audit logs. | Submission | Audit Logging |
| The system must log when a submission is created to the audit logs. | Submission | Audit Logging |
| The system must log when a user changes their login name to the audit logs. | Submission | Audit Logging |
| The system must log when a user changes their first/last name to the audit logs. | Submission | Audit Logging |
| The system must log when a user changes their phone number to the audit logs. | Submission | Audit Logging |
| The system must log when each step of the submission wizard is visited to the audit logs. | Submission | Audit Logging |
| The system must log when a user account is locked, and the reason for the lock, to the audit logs. | Submission | Audit Logging |
| The system must log when a user account is unlocked to the audit logs. | Submission | Audit Logging |
| The system must log when a user account status is changed to the audit logs. | Submission | Audit Logging |
| The system must log when a CoR is downloaded to the audit logs. | Submission | Audit Logging |