Technical Requirements

2.0	NH eCourt Technical Requirements	Priority (M- Mandatory, D - Desired, F - Future)
2.1	**General Requirements**	
	The application does not require any Plug-ins / Active X controls	D
	The application does not require any client side installs. (zero foot print without dependencies)	D
	The application must support a wide variety of browsers including and not limited to: Microsoft Internet Explorer 6.x and later, Firefox Google Chrome, and Safari	M
	Session duration shall be configurable	D
	Rights and privileges shall be assigned to users, groups and roles by an administrator.	M
	The user interface shall dynamically reflect functions and capabilities that are consistent with the user's rights and privileges.	M
	Basic activity logging, recording and storage functionality to be configured. The solution should maintain logs of all user activity. Archival logging to be configured.	M
	The application should provide a configurable user interface layer that will allow for site branding.	D
	The system shall provide integration with the court supported e-mail system.	D
	The response time for any data query shall be 3 seconds from the web portal & 1 second from internal application.	D
	The response time for any image query data shall be 3 seconds from the web portal & 1 second from internal application	D
	The response time for data inserts or updates shall be 3 seconds from the web portal & 1 second from internal application	D
	The system shall provide processing visual displays indicating that the system is in the process of responding to the user's request. Include status bar % complete. Individual percentages should be displayed for multiple uploads.	D
	The system shall prevent inadvertent multiple processing such as a user clicking a submit button twice.	M
	System will support limiting quotas for file sizes, etc.	D
	The application can be re-deployed in whole or in part from a SaaS model to a traditional model with a low impact conversion effort.	D
	Any software upgrades will be backward compatible with existing interfaces.	M
	Core application functionality can be deployed natively on mobile OS such as iOS, Android and Windows Phone. Please explain current abilities and future plans.	F
2.2	**Application Security**	
	The application shall support a mixed authentication mode of either application security, LDAP, or AD.	D
	The application shall support LDAP-v3 compliant directories for authentication.	M
	The application shall support active directory for authentication.	M
	Login credentials shall be encrypted	M
	The application shall support strong password techniques	M
	The application shall support configurable password strength rules. These rules must account for password length, character combinations and patterns, upper and lower case letters, numbers and special characters.	M
	The application shall support configuration of password reset frequency. (None or xx days)	M

2.0	NH eCourt Technical Requirements	Priority (M- Mandatory, D - Desired, F - Future)
	The application shall support automatic inactivating of accounts based on configurable inactivity periods.	M
	The application shall support password validation rules based on profile data such as identifiers, phone numbers, addresses, login id and email address.	M
	The application shall support password validation rules based on configurable history of previous passwords.	M
	The application shall provide a secure mechanism for password resets. Examples would include security question challenges, emailing of temporary password, emailing of notification of changed profile, etc. A multiple approach password scheme would be preferable. Please explain the applications capabilities.	M
	The application shall support virus scanning and malware with latest definitions of all uploaded documents	M
	The application shall support both a manual and automatic registration process.	M
	The application shall support role based security.	M
	The application is safe guarded against Sql vulnerabilities.	M
	The vendor will follow best data loss prevention practices	M
2.3	**Standards**	
	The application provides the following ECF 4.0 conformant operations: GetPolicy, GetServiceInformation, GetFeesCalculation, ReviewFiling, ServeFiling, RecordFiling, NotifyDocketingComplete, NotifyFilingReviewComplete, GetFilingList, GetFilingStatus, GetCaseList, GetCase, GetDocument	D
	The application provides the ability to deploy the ESFP and EFM as one application or separate applications.	D
	The application supports Hypertext Transfer Protocol (HTTP)	M
	The application supports Secure (HTTPS)	M
	All API exposed for integration with other application shall be Web Services conforming to Industry Standards	M
	The application supports Simple Object Access Protocol (SOAP) 1.2	M
	The application supports Universal Description, Discovery and Integration (UDDI)	D
	The application provides Web Services Description Language (WSDL) for all of its interfaces	M
	The application supports NIEM 2.0 for its message schemas.	D
	The application complies with United States Section 508	M
	The application complies with Web Content Accessibility Guidelines (WCAG) 2.0.	M
	All financial transactions must be PCI Compliant.	M
2.3	**Data Center**	
	The data center must provide secured access and video monitoring (CCTV)	M
	The data center must provide access doors with audible alarms	M
	The data center must provide computer based access system with badge or biometric readers	M
	The data center must provide anti pass-back (badge-out) functionality preventing badge sharing	M
	The data center must provide sufficient generator and UPS battery backup	M
	The data center must provide redundant power supply	M
	The data center must provide fully redundant data center grade cooling system	M
	The data center must provide early fire detection system	M
	The data center must provide cascading site design to segregate fire damage.	D
	The data center must provide smoke detection system	M

2.0	NH eCourt Technical Requirements	Priority (M- Mandatory, D - Desired, F - Future)
	The data center must provide advanced leak and water detection system	M
	The data center must provide must provide 99.9% uptime 24X7, 365	M
	The data center must provide intrusion protection system (IPS)	M
2.4	**Software as a Service (SaaS)**	
	The hosting provider shall follow the Data Center requirements found in section 2.3.	M
	The hosting provider shall have passed SAS 70 Type I and Type II Certifications	D
	The application site supports File Transfer Protocol Secure (FTPS)	D
	The application site supports File Transfer Protocol (SFTP)	D
	All network traffic between the browser and the application shall be encrypted.	M
	The hosting provider will also provide a test and staging environment of the application.	M
	The hosting provider will provide a SAAS environment that is segregated from other implementations. (Single instance, not multi-tenancy)	M
	In the event of a planned or unplanned outage, service provider must supply an outage notice on the website.	M
	The SaaS provider must provide data and system backups stored in a remote location.	M
	The SaaS provider must provide technical management reports including bandwidth and storage utilization.	M
	The SaaS provider must provide 72 hour response time to capacity increases to memory and storage.	D
	The hosting site must provide an Active-Active High Availability configuration	M
	The hosting provider must provide monitoring tools to detect and alert suspicious activity such as Phishing.	M
	SaaS provider is responsible for all Operation System maintenance including periodic patches.	D
	SaaS provider is responsible for all Database maintenance.	D
	SaaS provider is required to notify the State when any third party requests access to data (e.g., Patriot Act).	D
	SaaS provider will provide Service Level Agreement options and associated costs.	M
	SaaS provider will provide change management options and associate costs	M
	System will support the addition of other active cases that are currently paper based.	D
2.5	**Technical Deployment**	
	The application can support an Active-Active High Availability configuration.	M
	The application can be deployed on Windows Server 2012 or Linux-based environment.	M
	The application can run on 32bit and 64 bit operating systems.	M
	The application is certified to run on SQL Server 2012 or ANSI-compliant database	M
	The application is certified to run on virtual platform.	M
2.6	**Document Management**	
	The DMS shall support TWAIN (2.1) software protocol.	M
	The DMS shall support storage of content on Storage Area Networks (SAN)	M
	The DMS shall provide web services based interfaces for storage and retrieval.	M
	The DMS shall support role based security so to only authorized users will have access to documents and electronic assets in both user interfaces and web services.	M
	The solution supports integration with 3rd party Document Management Systems that are not imbedded in the core solution.	D
	The DMS shall natively support the storage and display of all the common file formats including but not limited to HTML- JPEG, TIFF, -RTF, PDF, PDFA, Text, MS Word, MS Excel, etc..	M

2.0	NH eCourt Technical Requirements	Priority (M- Mandatory, D - Desired, F - Future)
	The DMS shall support URL retrieval of documents.	D
	The DMS shall support mass uploads of documents and indexes.	M
	The DMS application shall support MS SQL Server 2012 & ANSI-compliant databases.	M
	Solution shall support conversion of scanned images into searchable PDF.	M
	The system shall support integrations with multiple best-of-breed forms processing packages for advanced forms processing and automated indexing	D
	The DMS should support a configurable data retention policy that is comprehensive to both data and images.	D
	The DMS shall support a multi-tiered storage strategy. This will allow current documents to be stored on one tier and archived documents on another.	D
	The DMS shall support retrieval from a multi storage configuration. This configuration will allow current documents to be retrieved faster than archived documents on a different storage tier.	D
	Any storage tier can be segmented into small storage structure. This will allow for easier management of backup and recovery of each storage structure.	D
	The DMS shall provide a management console for DMS basic and storage configuration.	M
	The DMS shall provide the ability to render images in PDFA format.	D
	Vendor will describe migration approach to best in class DMS (e.g., DoD 5015 DMS)	D
2.7	**Mobile Device Management(MDM)**	
	MDM solution shall provide an easy to use administration console.	F
	MDM solution shall provide for a secured application container.	F
	MDM solution shall allow for disabling a users access.	F
	MDM solution shall all for remote application disabling and removal from mobile device.	F
	MDM solution shall allow for downloading of approved applications and application updates from central library	F
	MDM solution shall be scalable to accommodate thousands of users.	F
	MDM solution shall be deployable on-premise or in a SaaS model.	F
	MDM solution shall encrypt data travelling from server to device.	F
	MDM solution shall provide strong security support through a multilayer defense approach that encompasses users, devices, applications, files and content, and connections that include Federal Information Processing Standard (FIPS) and other certifications	F
	MDM solution shall provide analytical reports and dashboards.	F
	MDM solution shall provide ability to integrate with Active Directory.	F