	Appendix A - Business Requirements	Priority M - Mandatory D - Desired
1	**Who**	
1.1	The system must provide the capability to restrict user access to specific cases in Odyssey to active Odyssey case parties only (excluding participants) based on party type (connection to the case). ****Active parties might need to be excluded from accessing case information through the system.** ****Active parties, when changed to "inactive parties" or "participants", should no longer have the "active party" access they previously had in the system.**	**M**
1.2	The system must provide the capability of displaying selected case related information based on user types, party types and/or account types.	**M**
1.3	The system must provide the capability to extend Odyssey security settings to the system. For example: **No system users can access cases in Odyssey case security group "A", but some system users may access cases in Odyssey case security group "B". **No system users can access documents in Odyssey document security group "X", but some system users may access documents in Odyssey document security group "Y". **No system users can access party mailing addresses marked in Odyssey as "confidential".	**M**
1.4	The system must provide the capability to identify agencies and attorneys that can provide authorized access to non-parties to selected cases. Responsibility of maintaining this authorized access will lie with the agency/attorney. (For example Firm Admin)	**D**
1.5	The system must provide the capability to set, by account type, a configurable limit to the search results returned as well as the number of case summaries available.	**M**
1.6	The system must provide the capability for search criteria to be configurable based off account type.	**M**
2	**What**	
2.1	The system must provide to the user a dashboard of all cases to which they have been granted access to through the system. **Both an automatic (configurable) & manual solution, to grant access to various cases in the system, should be made available**	**M**
2.2	The system must provide the capability to filter cases within the dashboard by: case#, filing date range, case status, case type, odyssey case style (wildcard search), hearing date, party name, and/or court	**M**
2.3	The system must provide online FAQ functionality for application use and business policy matters	**M**
2.4	The system must provide an online user manual for the application	**M**

2.5	The system must provide the capability to have online help accessible from each screen of the application	**M**
2.6	The system must provide configurable quick links. For example, a quick link to the eFiling system (application for users to file cases electronically with the courts) and a quick link to general NHJB information with directions, maps and phone numbers for all courts in NH	**M**
2.7	The system must be configurable to link future online services offered by the NHJB (e.g. online fine payment application)	**M**
2.8	The system must provide functionality to view , save (in pdf format) and print case filings/documents	**M**
2.9	The system must be accessible from the kiosk located in the courthouse, and remotely through the internet, to the extent allowed by NHJB policy (TBD) and applicable statutes.	**M**
2.10	The system must be accessible from the kiosk located in the courthouse, with functionality allowing the court to switch the system on and off, on demand.	**D**
2.11	The system must provide functionality for configuration of emails sent from the application	**M**
2.12	The system must provide the capability to make documents viewable by case type and event type, and make viewable only those documents attached to specified event types.	**D**
2.13	The system must reflect the accurate time/time zone	**M**
2.14	The system must display when the data was last refreshed	**M**
2.15	The system must display complete and accurate information from our case management system	**M**
2.16	The system must have the ability to distinguish between local public access and internet public access to determine what case types and/or document security types are available in a court house lobby vs global access. (i.e. Guardian cases are available to the public in the court house lobby but not elsewhere)	**M**
3	**Reporting**	
3.1	Application shall have the ability to run a report of all users and their activity	**M**
3.2	Application shall have the ability to run a report containing information on account types including access and permissions that have been granted	**D**
3.3	Application shall have the ability to run a report of all configuration changes which will be triggered when change is made	**D**
3.4	Application shall have the ability to report on all application data	**M**

	Appendix A - Technical Requirements	Priority M - Mandatory D - Desired
4	**Integration**	
4.1	The application must integrate with the NHJB’s Odyssey case management system (CMS) through the NHJB’s existing service layer utilizing RESTful APIs.	**M**
4.2	The electronic exchange of data should conform to the US DOJs Global Reference Architecture (GRA) standards, as practical.	**M**
4.3	This electronic data exchange should be completely automatic in that it should happen in the background, using the NHJB Service Layer while the court staff continues to process cases in Odyssey, as they do currently.	**M**
4.4	Ability to implement JWT token authentication for web service calls.	**M**
4.5	All web service calls and redirects must use HTTPS protocol.	**M**
4.6	Provide transactional audit of requests and responses	**M**
5	**Registration**	
5.1	Application shall have central administration capability to add, edit and delete party and court users/staff access with appropriate rights management - specific court & IT Staff	**M**
5.2	Application shall have a capability to allow/reject registration based on business rules that can be configured.	**M**
5.3	Application shall have a capability for the specific court & IT staff to approve or reject new registrations.	**M**
5.4	Application shall be able to send automated emails (send a confirmation email after a party has registered successfully with Application etc.) If SMTP is utilized than custom port and security settings shall be configurable by the application.	**M**
5.5	Application shall perform verification prior to registration. (Examples: Email, Text Message)	**M**
5.6	Application shall perform auto registration for the case initiator using the filers email address	**D**
6	**Security and Access Rights Management**	
6.1	Application shall provide a capability to enforce two factor authentication for incoming login requests after user id and password authentication for certain account types.	**M**
6.2	Application shall impose an account lock-out after three unsuccessful login attempts. Lock-out period shall be configurable in regards to amount of login attempts and duration of lock out.	**M**
6.3	Application shall provide a capability for registered users to retrieve a user id or reset a password via email along with additional utilizing 6.1 dependency (two factor authentication)	**M**
6.4	Application shall provide strong password authentication by configurable rules that must account for password length, character combinations and patterns, upper and lower case letters, numbers, and special characters. Should support common dictionary check and store password history.	**M**

6.5	Application shall impose a password expiry time that shall be configurable. Default should be 180 days.	**M**
6.6	Application upon password change shall require user to enter current password, prior to accepting new password and send email to the user upon password change.	**M**
6.7	Application shall encrypt passwords and prevent passwords from being displayed or printed. Login credentials shall be encrypted. Application shall not store unencrypted application or system passwords in plain text, xml, json, or any other configuration file on any server.	**M**
6.8	Application shall provide safe guards to ensure that a user, once authenticated, can view only data they are authorized to access.	**M**
6.9	Application shall provide a capability to ensure that confidential information on any displayed page is only viewable by users with the required authorization.	**M**
6.10	Application shall use and be configured with HTTP Strict Transport Security (HSTS) standards.	**M**
6.11	Application shall provide a capability to log events to Syslog.	**M**
6.12	Application shall have security and control features that detect and prevent unauthorized access to the application	**M**
6.13	Application shall allow security configuration changes made by security administrators to take effect immediately or at a specified time.	**M**
6.14	Application shall provide a capability for security administrators to terminate user's sessions immediately.	**M**
6.15	Application shall provide a capability to define security administrator user management functionality in granular fashion.	**M**
6.16	Application shall support and implement Lets' encrypt certificates and configurations.	**M**
6.17	Application shall support one or more mixed authentication modes for administrator accounts such as application security, standalone,LDAP-v3, Active Directory, and/or token authentication.	**M**
6.18	Application shall provide secure maintenance area. Application shall display a configurable notice to all users that the application is unavailable; however, still allows designated application administrators access.	**M**
6.19	Application shall safe guard against application and database vulnerabilities including; however, not limited to session management, authorization and access control, authentication, data and input validation, buffer overflows, insecure use of cryptography, and application/server misconfigurations	**M**
6.21	Any data communication between browser and application shall be encrypted.	**M**
6.22	All application including front and/or backend operations and/or data between servers shall be encrypted.	**M**
6.23	Application session duration shall be configurable	**M**
6.24	Application shall display appropriate informational error pages for end users without revealing application or system information.	**M**
6.25	Application shall require two factor authentication for all administrative sessions	**M**
6.26	Application shall allow user to update their own login email	**D**
6.27	Application shall update changes to users access in real time	**D**

7	**Audit Trail**	
7.1	Application shall log all successful(including log in and log outs) or failed authentication attempts along with password change requests or any other third party vendor connection requests to Application including date/time, IP address, browser type, version and other pertinent information.	**M**
7.2	Application shall log all authenticated user actions requiring auditing based on business rules. Logging shall include; however, not limited to action date/time, user who performed the action, success or failure of action taken or changes made, business entities affected by this action, field values before and after changes are made, any other resources being authorized, etc.	**M**
7.3	Application shall allow authorized users to search and view the audit log as well as any archived audit logs.	**M**
7.4	Application shall provide a capability to determine who did what and when for any add, change, delete actions performed in the application	**M**
7.5	Application shall log all administrator activity, deletion of data, modification to system permissions, configurations, etc.	**M**
8	**Framework**	
8.1	Application shall not depend on any Plug-ins / Active X controls / Frameworks to pre-exist on client devices	**M**
8.2	Application shall not require any client side installs. (zero foot print without dependencies)	**M**
8.3	Application shall be cross-platform and entirely browser based	**M**
8.4	Application shall be HTML 5.0 (or latest version) compliant with a responsive web design	**M**
8.5	Application shall comply with United States Section 508	**M**
8.6	Application shall comply with Web Content Accessibility Guidelines (WCAG) 3.0.	**M**
8.7	Application shall provide a configurable and searchable audit log based on year, month, day, and time with ability to archive logs. Application shall have ability to import and export any logs on demand.	**M**
8.8	Application shall provide Web Services Description Language (WSDL) for all of its interfaces	**M**
8.9	The vendor shall follow best data loss prevention & redundancy practices	**M**
8.10	Application shall provide a message of the day notification	**M**
8.11	The application shall support Active-Active high availability configuration	**M**
8.12	The application shall display a progress bar for documents being rendered with actual percentage of completion	**D**
8.13	The application shall have a responsive design (i.e. Mobile device ready)	**M**