# APPENDIX A: Performance Requirement Summary

| PERFORMANCE REQUIREMENTS SUMMARY  **Case Management Systems Office** | | |
| --- | --- | --- |
| ***BPA Call Section*** | ***Performance Standard and AQL*** | ***Quality Assurance Method*** |
| C.4.1.1. System Availability – Upper Environments | 1. The Contractor shall ensure that each application is fully functional in the production, demo and training instances and that downtime is limited to less than the following hours per month. The downtime of each application and instance is measured independently and the failure to reach any AQL will result in a negative incentive.  Base Year  PACTS: 4 hours  All Other Probation Applications: 6 hours cumulative  Option Year #1  PACTS: 2 hours  All other probation applications: 4 hours cumulative  Option Year #2, #3, #4  PACTS: 1 hours  All other probation applications: 2 hours cumulative | Downtime occurs when any application or system component experiences a loss of functionality for core users. Downtime ends when the business owner of the application determines that full functionality has been restored to core users, they will notify the COR and Contractor via email. |
| C.4.1.1 System Availability – Lower Environments | The Contractor shall ensure that each application is fully functional in the Integration, Testing, and Staging instances and that downtime is limited to less than the following hours per month. The downtime of each application and instance is measured independently and the failure to reach any AQL will result in a negative incentive.  Base Year  Probation Applications: 12 hours, CM/ECF: 12 per court type  Option Year #1  Probation Applications: 8hours, CM/ECF: 8 per court type  Option Year #2, #3, #4  Probation Applications: 4 hours, CM/ECF: 4 per court type | Downtime occurs when any application or system component experiences a loss of functionality for core users. Downtime ends when the business owner of the application determines that full functionality has been restored to core users, they will notify the COR and Contractor via email. |
| C.4.1.1.2 Data Integrity/Availability | 1. Contractor shall ensure zero data loss occurs at any time in any area of the upper environments 2. Contractor shall ensure production data remains accessible to the user community at all times within each of the upper environments. 3. Contractor shall ensure zero code development and application configuration loss occurs at any time in all upper and lower environments. | Data loss occurs when any user is unable to access data submitted into any of the upper environment systems while services are available.  Code development loss occurs when any developer is unable to access developed code submitted into an upper or lower environment system repository while those system repository services are available.  Application configuration data loss occurs when a system administrator is unable to reinstall, install, or configure an application on a new or existing server or system to restore normal operations within 1 business day. |
| C.4.2.1. Availability of Help Desk personnel to respond to incoming tickets | Contractor shall ensure that Help Desk staff is available to assist users during duty hours (0700-1730 EST) such that 98% of the tickets received have technical actions taken upon within in 1 business day. If a ticket is received after 4:00 PM EST it must be acted upon by noon the following business day. All tickets must be resolved within 72 hours or escalated as appropriate. | COR Monitoring and Customer Complaints |
| C.4.2.2. Identify New Releases and Service Patches. | 1. The Contractor shall provide to the COR the information described in SOW Section C.4.2.2 and within 3 days of the release to the public.  2. The Acceptable Quality Level (AQL) for this standard is 10 days. | COR Monitoring |
| C.4.3.1 Security Operations Management Support. | The Contractors shall maintain that all servers are properly patched to within 60 days of a patch release.  The Contractor shall maintain that all servers are properly patched to within 1 week of a zero-day patch release.  The contractor shall insure all servers are connect to the Enterprise SPLUNK Server  The contractor shall insure all servers are running current anti-virus software. | ISSO Monitored and reported to the COR |
| C.4.3.2 Cyber Security Defense | The Contractors shall update all zero-day patches within one week of being notified by ITSO. | ISSO Monitored and reported to the COR |
| F-1 Deliverables | 1. Contractor shall provide all deliverables in accordance section F-1 Deliverables.   AQL is not more than 5 workdays late. | COR Review for timeliness and thoroughness. |