Security requirement

1. Build the system Use n-tier architecture (web, application, database)
2. The system should support (strong password, account lockout/captcha) and Should support integration with 2FA
3. Ensure secure messaging/web services/API according to the WS-Security Standard or and OWASP
4. Design and build encrypted secure connections and communication channels to ensure:
    - Secure connections between clients and the System.
    - Secure connections between the System and it is component
5. The system should support Role-based access control (RBAC) where the systems can assign access and actions according to a person's role within the system in addition to that a map of role should be developed for the solution.
6. The solution should include comprehensive audit and log management for all transactions/activity/changes, especially security logs, based on need-to-know and need-to-do
7. Ensure that all the servers (web , application and database) are Configure using the security best practices
8. Conduct vulnerability assessment and penetration test for the solution and the mobile application through a third party (the third party company should be approved by hcst/mode

hcst/MoDEE reserves the right to perform their own vulnerability assessment and/or penetration test on the solution and provide the vulnerability reports to the winning bidder to apply appropriate recommendations to ensure system security. Another security test should be conducted to ensure recommendations are reflected.