# Title: Sample Set for Non-Functional Requirements

1. **Security:**
    a. The portal should undergo regular security audits and penetration testing.
    b. Access to sensitive data and administrative functions should require multi-factor authentication (MFA).
    c. System must be compliant with NIST and GSA's 2100 Security Policy
    d. System will control features and data via roles based access for users

2. **Compliance:**
    a. User data should be handled in compliance with relevant data privacy laws and regulations.
    b. User consent mechanisms for data collection and processing should be in place.
    c. 508 Compliant
    d. The portal must comply with relevant government regulations, such as HIPAA, FISMA, or FedRAMP.
    e. It should also adhere to web accessibility standards, such as WCAG 2.1.
    f. It should ensure compliance with policy requirements such as FAR, GSAR, GSAM, clause logic based on different program type

3. **Architecture & Design:**
    a. Data Architecture
    b. Software architecture and frameworks
    c. Session state management
    d. Platform specific configurations

4. **System Hosting:**
    a. Any server, real or virtual, network, Internet connection, infrastructure, hardware and applications used to host Software.
    b. Verify the hosting of all application software, databases, computer network communications equipment, security applications and system software on computer equipment controlled by the Contractor by reviewing the Supplier Portal system design documentation.

5. **Monitoring and Alerting:**
    a. Real-time monitoring should be set up to detect and respond to performance issues, security breaches, and downtime throughout the essential business processes.

6. **Logging and Auditing:**
    a. All user (internal and external) interactions and system activities must be logged and audited for security and compliance purposes.
    b. Logs should be retained as determined by GSA's policy requirements.

7. **Backup Methods:**

a. Regular automated backups of all data should be performed based on requirements determined by policy.

8. **Reliability, Maintainability, & Availability:**
    a. The portal should have a minimum uptime of 98.5% excluding scheduled maintenance, and any other external dependencies.
    b. Scheduled maintenance windows should be communicated to users at least 48 hours in advance.

9. **Disaster Recovery:**
    a. Verify Supplier Portal provides a failover/disaster recovery capability in the event of any failure in accordance with contractual SLAs.
    b. Operational processes must be in place to avoid risk of data loss.

10. **Browser Configuration:**
    a. The portal should be compatible with the latest versions of major web browsers (e.g., Chrome, Firefox, Edge, Safari), identified by GSA.
    b. Verify Supplier Portal does not use persistent cookies on the user's machine.

11. **Performance:**
    a. Load balancing should be implemented to distribute incoming traffic evenly across platform services, native cloud and user scalability.
    b. The portal must load within 2 seconds on average for users
    c. Response times for critical functions (e.g., submitting offers) should be less than 1 second or negotiable as applicable

12. **Contractor Onboarding Process:**
    a. GSA system data/specifications will not be provided to the contractor until adjudicated
    b. Contractor should be compliant and efficient to onboard/offboard resources

13. **Usability:**
    a. The user interface incorporates data entry features designed to reduce the amount of direct keying required to initiate the processing. Desired efficiencies include the use of default values, look-up tables, and automatic data recall.

14. **Product Support:**
    a. Contractor will be responsible to maintain and operate the system, based on GSA's defined regulations, guidance, and principles.