ISS Technology RFP Check List

Please provide responses to the following questions. If needed, attach additional pages to provide responses. For questions that are not applicable, mark "N/A" *and* explain why the question is not applicable.

#	Security Questions	Response
SEC 1.1	Are you able to provide the solution for UC operating system vulnerability scans?	
SEC 1.2	What are your authentication protocols?	
SEC 1.3	Describe SSO solutions and ability to integrate with SAML solutions including Shibboleth, Okta, Microsoft ADFS and Azure AD.	
SEC 1.4	Describe Application Access Audit and monitoring capability.	
SEC 1.5	Describe any server/application configuration options for security (i.e. timeout, lockout).	
SEC 1.6	Describe how security configuration is managed for hardware and/or software (including OS).	
SEC 1.7	Provide Security risk/vulnerability assessment Results.	
SEC 1.8	Describe continuous security vulnerability assessment & Remediation process.	
SEC 1.9	Describe methodology on staying current with latest security standards.	
SEC 1.10	Describe Security Patch process.	
SEC 1.11	Describe authenticated (Privileged) scan process.	
SEC 1.12	Describe User Account provision/de-provision/change Process (include infrastructure, configuration management and software).	
SEC 1.13	Describe User Account review process.	
SEC 1.14	Describe intrusion detection process.	
SEC 1.15	Describe password mandates.	
SEC 1.16	Describe data encryptions for all sensitive data.	
SEC 1.17	Describe password/passphrase complexity.	
SEC 1.18	Describe encryption in Transit between all devices and servers.	
SEC 1.19	Describe encryption on Mobile devices and removable storage media.	
SEC 1.20	Describe secure deletion process upon decommission.	
SEC 1.21	Describe control access to the application via its incorporated interface.	

ISS Technology RFP Check List

SEC 1.22	Describe control access to the underlying data via direct and third-party tools.	
SEC 1.23	Describe control access across different user roles.	
SEC 1.24	Describe security at the field level, screen level and user role level.	
SEC 1.25	Describe privacy and security training in your organization.	
SEC 1.26	Describe reports available for all audits within the system.	
SEC 1.27	Describe data encryption for all restricted data at rest.	
SEC 1.28	Describe data encryption for all restricted data during process.	
SEC 1.29	Describe key management capabilities and lifecycle (key storage, use, distribution, destruction, archiving, offline availability, generation, etc.).	
SEC 1.30	Describe encryption algorithms.	
SEC 1.31	Describe key exchange capabilities.	
SEC 1.32	Please describe Active Directory integration and support capabilities (leverage LDAP, Active Directory services, forest aware, federated services, non-contiguous DNS domain Active Directory forest of trees, etc.).	
SEC 1.33	Describe user account provisioning API's and automation capabilities.	
SEC 1.34	Describe HIPAA compliance with the security rule administrative safeguards (required and addressable elements).	
SEC 1.35	Describe HIPAA compliance with the security rule technical safeguards (required and addressable elements).	
SEC 1.36	Describe HIPAA compliance with the security rule physical safeguards (required and addressable elements).	
SEC 1.37	Describe your companies risk analysis and risk management processes.	
SEC 1.38	Describe any audit or certification (e.g. SOC 2 type 2, ISO, etc.).	
SEC 1.39	Describe PCI compliance capabilities.	
SEC 1.40	Describe FERPA compliance capabilities .	
SEC 1.41	Describe adherence to SB1386 regulatory compliance.	
SEC 1.42	Describe user ID/password expiration options (date based, lack of activity based, brute force	

	lock out) and if the solution can meet UC policies and standards.	
SEC 1.43	Does the solution require password changes? Please describe.	
SEC 1.44	Does the service offer self-service for user based password self-service and/or security questions? Please describe.	
SEC 1.45	Can your solution provide automatic logoff based on time and/or activity? Please describe.	
SEC 1.46	Can you solution provide login activity (frequency and anomaly detection? Please describe.	
SEC 1.47	Can you solution provide login geographic anomaly detection? Please describe.	
SEC 1.48	Does your solution provide two-factor authentication, partner-based integration with another two-factor authentication solution or a best practice integration reference.	
SEC 1.49	Are passwords masked when entered in the password field? Please describe.	
SEC 1.50	Are passwords removed on page reload or when selecting the "back button"? Please describe.	
SEC 1.51	Does the solution provide user activity reporting? Please describe.	
SEC 1.52	Does the solution provide administrative roles based access control with pre-built templates? Please describe.	
SEC 1.53	Does the solution provide user-based roles based access control with pre-built templates? Please describe.	
SEC 1.54	Describe login auditing detail available in solution.	
SEC 1.55	Does the solution provide external/federated authentication or public userID capabilities? Please describe.	
SEC 1.56	Is data encrypted between application tiers and/or different elements of a distributed system (e.g. encrypted when transmitting information between the web server, the application server, and the web server)? Please describe.	
SEC 1.57	Does the solution offer offline media encryption? Please describe.	
SEC 1.58	Describe the log retention capabilities.	

ISS Technology RFP Check List

SEC 1.59	Please describe the system recovery options for the solution and any customer provided pre-requisites.	
SEC 1.60	Does the vendor provide documentation describing best practice architecture and guidance for various recovery time objectives and recovery point objectives?	
SEC 1.61	Please describe the software development lifecycle model and or any standards followed in creating, maintaining, and versioning software.	
SEC 1.62	Please describe adherence to development for best practices and to mitigate common vulnerabilities such as XSS, XSRF, SQL injection, etc.	
SEC 1.63	Please describe programming practices to protect against buffer overflows, format string attacks, in-memory data exfiltration attacks, etc.	
SEC 1.64	Please describe reference deployment/architecture/configuration penetration and vulnerability testing.	
SEC 1.65	Describe your SDLC process security assurance activities.	
SEC 1.66	Describe your “High Availability and Disaster Recovery” features for SaaS model solution offering.	

#	IT Security Controls	
1	Describe your Mobile app deployment (Apple App store, Google Play etc.) methodology.	
2	Describe your mobile app Authentication with respect to strong authentication (PIN etc.) and/or Mobile integrated “Touch ID” features to ensure identity of user and non-repudiation.	
3	Describe Encrypted communication between user (patient) and UC Health systems to address data in motion security.	
4	Describe your “access controls /monitoring/alerting” in place to address any potential unauthorized access violation that can be caused by privileged accounts such as Administrative and Service Accounts within your SaaS offering, which may circumvent “SAML/Single Sign on/ Shibboleth integration” type controls we may implement.	

ISS Technology RFP Check List

5	If applicable, describe how you will securely remote connect to an on-premises hosted infrastructure configuration/maintenance model.	
6	Describe your HIPAA compliant infrastructure security controls.	
7	Do you have a published Information Security/protection Management Program and dedicated IT security team?	
8	Describe how your SaaS solution takes advantage of CASB (Cloud Access Security Broker) to address / prevent unauthorized data leak scenarios.	
9	Describe “Data Isolation” controls to safeguard our organizations data in your shared tenant SaaS solution.	
10	Describe Data at Rest – security controls with respect to encryption in your SaaS offering.	
11	Describe your logging features and natively supported SIEM solutions with which it integrates.	
12	Describe DDOS protection controls in place to protect your SaaS solution.	
13	Describe how our SaaS solution is taking advantage of WAF (Web Application Firewall) and potential to integrate with our organization’s WAF protection, if you don’t have one in place today.	