Security Requirements for 511DFW

1. INTRODUCTION

The selected firm(s) and the Project Review Committee (PRC) agree to maximize the security of the software according to the following terms.

2. PHILOSOPHY

This section is intended to clarify the security-related obligations of the PRC and the selected firm(s). At the highest level, the parties agree that:

(a) Security Decisions Will Be Based on Risk

Decisions about security will be made jointly by both the selected firm(s) and the PRC based on a firm understanding of the risks involved.

(b) Security Activities Will Be Balanced

Security effort will be distributed across the entire software development lifecycle.

(c) Security Activities Will Be Integrated

All the activities and documentation discussed herein can and should be integrated into the firm(s)' software development lifecycle and not kept separate from the rest of the project. These requirements do not imply any particular software development process.

(d) Vulnerabilities Will Be Addressed

All software has bugs, and some of those will create security issues. The selected firm(s) will strive to identify and address vulnerabilities as early as possible in the lifecycle.

(e) Security Information Will Be Fully Disclosed

All security-relevant information will be shared between the PRC and the selected firm(s) immediately and completely.

(f) Only Useful Security Documentation Is Required

Security documentation does not need to be extensive in order to clearly describe security design, risk analysis, or issues.

3. LIFECYCLE ACTIVITIES

(a) Risk Understanding

The selected firm(s) and the PRC agree to work together to understand and document the risks facing the application. This effort should identify the key risks to the important assets and functions provided by the application. Each of the topics listed in the requirements section should be considered.

(b) Requirements

Based on the risks, The selected firm(s) and the PRC agree to work together to create detailed security requirements as a part of the specification of the software to be developed. Each of the topics listed in the requirements section below should be discussed and evaluated by both the selected firm(s) and the PRC. These requirements may be satisfied by custom software, third party software, or the platform.

(c) Design

The selected firm(s) agrees to provide documentation that clearly explains the design for achieving each of the security requirements. In most cases, this documentation will describe security mechanisms, where the mechanisms fit into the architecture, and all relevant design patterns to ensure their proper use. The design should clearly specify whether the support comes from custom software, third party software, or the platform.

(d) Implementation

The selected firm(s) agrees to provide and follow a set of secure coding guidelines and to use a set of common security control programming interfaces (such as the OWASP Enterprise Security API (ESAPI)). Guidelines will indicate how code should be formatted, structured, and commented. Common security control programming interfaces will define how security controls must be called and how security controls shall function. All security-relevant code shall be thoroughly commented. Specific guidance on avoiding common security vulnerabilities shall be included. Also, all code shall be reviewed against the security requirements and coding guideline before it is considered ready for unit test.

(e) Security Analysis and Testing

The selected firm(s) will perform application security analysis and testing (also called "verification") according to the verification requirements of the OWASP Application Security Verification Standard (ASVS) or another agreed upon standard. The selected firm(s) shall document verification findings according to the reporting requirements of the standard. The selected firm(s) shall provide the verification findings to the PRC.

(f) Secure Deployment

The selected firm(s) agrees to provide secure configuration guidelines that fully describe all security relevant configuration options and their implications for the overall security of the software. The guideline shall include a full description of dependencies on the supporting platform, including operating system, web server, and application server, and how they should be configured for security. The default configuration of the software shall be secure.

4. SECURITY REQUIREMENT AREAS

The following topic areas must be considered during the risk understanding and requirements definition activities. This effort should produce a set of specific, tailored, and testable requirements. Both the selected firm(s) and the PRC should be involved in this process and must agree on the final set of requirements.

(a) Input Validation and Encoding

The requirements shall specify the rules for canonicalizing, validating, and encoding each input to the application, whether from users, file systems, databases, directories, or external systems. The default rule shall be that all input is invalid unless it matches a detailed specification of what is allowed. In addition, the requirements shall specify the action to be taken when invalid input is received. Specifically, the application shall not be susceptible to injection, overflow, tampering, or other corrupt input attacks.

(b) Authentication and Session Management

The requirements shall specify how authentication credentials and session identifiers will be protected throughout their lifecycle. Requirements for all related functions, including forgotten passwords, changing passwords, remembering passwords, logout, and multiple logins, shall be included.

(c) Access Control

The requirements shall include a detailed description of all roles (groups, privileges, authorizations) used in the application. The requirements shall also indicate all the assets and functions provided by the application. The requirements shall fully specify the exact access rights to each asset and function for each role. An access control matrix is the suggested format for these rules.

(d) Error Handling

The requirements shall detail how errors occurring during processing will be handled. Some applications should provide best effort results in the event of an error, whereas others should terminate processing immediately.

(e) Logging

The requirements shall specify what events are security-relevant and need to be logged, such as detected attacks, failed login attempts, and attempts to exceed authorization. The requirements shall also specify what information to log with each event, including time and date, event description, application details, and other information useful in forensic efforts.

(f) Connections to External Systems

The requirements shall specify how authentication and encryption will be handled for all external systems, such as databases, directories, and web services. All credentials required for communication with external systems shall be stored outside the code in a configuration file in encrypted form.

(g) Encryption

The requirements shall specify what data must be encrypted, how it is to be encrypted, and how all certificates and other credentials must be handled. The application shall use a standard algorithm implemented in a widely used and tested encryption library.

(h) Availability

The requirements shall specify how it will protect against denial of service attacks. All likely attacks on the application should be considered, including authentication lockout, connection exhaustion, and other resource exhaustion attacks.

(i) Secure Configuration

The requirements shall specify that the default values for all security relevant configuration options shall be secure. For audit purposes, the software should be able to produce an easily readable report showing all the security relevant configuration details.

(j) Specific Vulnerabilities

The requirements shall include a set of specific vulnerabilities that shall not be found in the software. If not otherwise specified, then the software shall not include any of the flaws described in the current "OWASP Top Ten Most Critical Web Application Vulnerabilities."

5. PERSONNEL AND ORGANIZATION

(a) Security Architect

The selected firm(s) will assign responsibility for security to a single senior technical resource, to be known as the project Security Architect. The Security Architect will certify the security of each deliverable.

(b) Security Training

The selected firm(s) will be responsible for verifying that all members of the selected firm(s)’ team have been trained in secure programming techniques.

(c) Trustworthy Developers

The selected firm(s) agrees to perform appropriate background investigation of all development team members.

6. DEVELOPMENT ENVIRONMENT

(a) Secure Coding

The selected firm(s) shall disclose what tools are used in the software development environment to encourage secure coding.

(b) Configuration Management

The selected firm(s) shall use a source code control system that authenticates and logs the team member associated with all changes to the software baseline and all related configuration and build files.

(c) Distribution

The selected firm(s) shall use a build process that reliably builds a complete distribution from source. This process shall include a method for verifying the integrity of the software delivered to the PRC.

7. LIBRARIES, FRAMEWORKS, AND PRODUCTS

(a) Disclosure

The selected firm(s) shall disclose all third party software used in the software, including all libraries, frameworks, components, and other products, whether commercial, free, open-source, or closed-source.

(b) Evaluation

The selected firm(s) shall make reasonable efforts to ensure that third party software meets all the terms of this agreement and is as secure as custom developed code developed under this agreement.

Security Requirements for 511DFW

8. SECURITY REVIEWS

(a) Right to Review

The PRC has the right to have the software reviewed for security flaws at their expense at any time within 60 days of delivery. The selected firm(s) agrees to provide reasonable support to the review team by providing source code and access to test environments.

(b) Review Coverage

Security reviews shall cover all aspects of the software delivered, including custom code, components, products, and system configuration.

(c) Scope of Review

At a minimum, the review shall cover all of the security requirements and should search for other common vulnerabilities. The review may include a combination of vulnerability scanning, penetration testing, static analysis of the source code, and expert code review.

(d) Issues Discovered

Security issues uncovered will be reported to both the PRC and the selected firm(s). All issues will be tracked and remediated as specified in the Security Issue Management section below.

9. SECURITY ISSUE MANAGEMENT

(a) Identification

The selected firm(s) will track all security issues uncovered during the entire lifecycle, whether a requirements, design, implementation, testing, deployment, or operational issue. The risk associated with each security issue will be evaluated, documented, and reported to the PRC as soon as possible after discovery.

(b) Protection

The selected firm(s) will appropriately protect information regarding security issues and associated documentation to help limit the likelihood that vulnerabilities in operational software are exposed.

(c) Remediation

Security issues that are identified before delivery shall be fixed by the selected firm(s). Security issues discovered after delivery shall be handled in the same manner as other bugs and issues.

10. ASSURANCE

(a) Assurance

The selected firm(s) will provide a "certification package" consisting of the security documentation created throughout the development process. The package should establish that the security requirements, design, implementation, and test results were properly completed and all security issues were resolved appropriately.

(b) Self-Certification

The Security Architect will certify that the software meets the security requirements, all security activities have been performed, and all identified security issues have been documented and resolved. Any exceptions to the certification status shall be fully documented with the delivery.

(c) No Malicious Code

The selected firm(s) warrants that the software shall not contain any code that does not support a software requirement and weakens the security of the application, including computer viruses, worms, time bombs, back doors, Trojan horses, Easter eggs, and all other forms of malicious code.

11. SECURITY ACCEPTANCE AND MAINTENANCE

(a) Acceptance

The software shall not be considered accepted until the certification package is complete and all security issues have been resolved.

(b) Investigating Security Issues

After acceptance, if security issues are discovered or reasonably suspected, The selected firm(s) shall assist the PRC in performing an investigation to determine the nature of the issue. The issue shall be considered "novel" if it is not covered by the security requirements and is outside the reasonable scope of security testing.

(c) Novel Security Issues

The selected firm(s) and the PRC agree to scope the effort required to resolve novel security issues, and to negotiate in good faith to achieve an agreement to perform the required work to address them.

(d) Other Security Issues

The selected firm(s) shall use all commercially reasonable efforts consistent with sound software development practices, taking into account the severity of the risk, to resolve all security issues not considered novel as quickly as possible.