# Department of Veterans Affairs, Pre-Procedure Checklist Tool

## Review

|  |  |
| --- | --- |
| **Date:** | |
| **Developer:** | **Reviewer:** |
| **Item(s) to Review:** | |

## Review Checklist

|  |  |
| --- | --- |
| [ ] Does not contain source code that is never invoked during operation | [ ] Does not contain invalid URL or path references |
| [ ] Not subject to error handling vulnerabilities | [ ] Validates all input |
| [ ] Follows the secure failure design principle | [ ] Not vulnerable to SQL Injection |
| [ ] Not vulnerable to integer arithmetic issues | [ ] Does not allow command injection |
| [ ] Does not contain format string vulnerabilities | [ ] Does not have cross site scripting vulnerabilities |
| [ ] Does not use hidden fields to control user access privileges or as a part of a security mechanism | [ ] Does not have buffer overflows, use functions known to be vulnerable to buffer overflows and does not use signed values for memory allocation |
| [ ] Cleans up resources after use | [ ] Does not have CSRF vulnerabilities |
| [ ] Not vulnerable to race conditions | [ ] Not vulnerable to XML Injection |
| [ ] Does not use global variables when local variables could be used | [ ] Does not have canonical representation vulnerabilities |
| [ ] Implements a simple solution | [ ] Design documents up to date and complete |
| [ ] Follows naming conventions |  |

## Review Notes

|  |
| --- |
|  |

## Follow up

|  |  |
| --- | --- |
| **Date:** | |
| **Developer:** | **Reviewer:** |

## Follow Up Notes

|  |
| --- |
|  |