|  |  |
| --- | --- |
| Assessment Information | |
| Application name |  |
| Version |  |
| Projected Start Date for Code Review |  |
| Desired End Date for Code Review |  |
| Has a source code analysis/scanner been performed against the application previously? If so, please provide any details available about the scan. |  |
| Language(s) used in development |  |
| What build tools are used? E.g. Ant or Maven for Java; Version of Microsoft Visual Studio for .NET |  |
| Number of Lines of Code1 |  |
| Number of Files |  |
| If this is an object oriented language, how many classes are defined in the application? |  |
| Is this a new or legacy application? If it is new, will multiple code reviews be required during the software development lifecycle, or prior to multiple releases of the application? |  |
| What is the average McCabe Cyclometric complexity value for the application?1 |  |
| What is the maximum McCabe Cyclometric complexity value for the application?1 |  |
| Are security requirements defined and available for the application? |  |
| Are misuse and abuse cases defined and available for the application? |  |
| Is software architecture and/or design documentation available? |  |
| Is a threat model available for the application? If no, does a threat assessment need to be performed? |  |
| A buildable application is required in order to scan the source code. Can all libraries, frameworks, dll’s, xml configuration files, make, Ant or Maven build files and any other 3rd party dependencies be provided with the source code? |  |
| Can the developers be contacted if there are problems with building the application? |  |
| Is a version control system used to manage the application source code? If yes, what VCS software tool is being used? |  |
| Does an Architectural Risk Assessment, which identifies architectural flaws with security implications, need to be performed? |  |

1SourceMonitor (<http://www.campwodsw.com/)> can be used to quickly analyze the lines of code and the McCabe Cyclometric complexity values for your source code. SourceMonitor measures metrics for source code written in C++, C, C#, VB.NET, Java, Delphi, Visual Basic (VB6) and HTML.

|  |  |
| --- | --- |
| Application Points of Contact (POC) | |
| Organization/Government primary POC: | Name: |
| Address: |
| Desk Phone |
| Mobile Phone/Pager: |
| E-mail: |
| Application technical POC: | Name: |
| Address: |
| Desk Phone |
| Mobile Phone/Pager: |
| E-mail: |

|  |  |
| --- | --- |
| Application | |
| Provide a brief summary of the application? What are some typical user transactions? |  |
| What type of users will be accessing this site? Employees? Veterans? Contractors? |  |
| What is the average number of users for the application per day? |  |
| How many user types and roles exist within the application? (e.g. user, administrator, auditor, helpdesk, etc.) |  |
| Does the website provide self-registration? Is admin approval of registered accounts required? |  |
| What type(s) of authentication are used or supported by application?(CAC, Windows AD, NTLM, simple HTTP, form based username and password, client certificate, etc.) |  |
| If application is divided into modules or sub-applications, provide short description of each and pertinent information about each (Approx size, user roles supported, languages used, additional authentication required, etc.) |  |
| Please attach application Flow/Usage diagrams or design documentation if available |  |
| What is the most important / sensitive information stored in the application? e.g. SSN, PII, PHI, Credit Card Numbers, etc. |  |
| What is the most damaging or dangerous action that could occur in the application? e.g. read only users can modify data, users can view other users’ credit card information, etc. |  |

|  |  |  |
| --- | --- | --- |
| Checklist for Software Required: | | |
|  |  | **The source code submitted must cleanly compile to an executable program.** |
|  | For a .NET application or any application built using Visual Studio, the following is required: the source code for the application (.cs files), as well as all libraries, frameworks, dll’s, xml configuration files, build files and any other 3rd party dependencies.   |  |  | | --- | --- | |  | Provide a zip file containing each Visual Studio solution’s top level directory and all subdirectories. For an ASP.NET application, with C# source files, this includes all .sln, .suo, .csproj, .cs, .aspx, .ascx, .asax, .asp, .config, .xml, .resx, .settings, .dll, .exe, .pdb, .txt, .cache, etc. files included in the Visual Studio solution and generated by Visual Studio. | |  | Any libraries (external .dll files) referenced by the solution, which are not included in the Visual Studio solution directory hierarchy must also be included. | | |
|  | For a Java application, the following is required: the source code for the application (.java files), the build script used to build the class, jar, and any executable files produced. This includes all of the Ant (build.xml) or Maven (pom.xml) build scripts for the Ant or Maven projects, as well as all libraries, frameworks, .jar files, xml configuration files, properties files, and any other 3rd party dependencies.   |  |  | | --- | --- | |  | Provide a zip file containing everything in the project’s Eclipse directory and workspace directory structures (or directory structure for the IDE used to develop and build the application). | |  | For Eclipse, provide the .metadata directory, or specific instructions for loading the workspace and projects into Eclipse, so that all projects can be compiled and built successfully. | | |

**WARNING: This document is FOR OFFICIAL USE ONLY. It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). This document is to be controlled, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public or other personnel without prior approval of the Veterans Affairs Chief Information Officer. Where appropriate, U.S. person identities have been removed. Should you have a requirement for particular U.S. person identity information, contact the VA-NSOC. No portion of this report should be furnished to the media, either in written or verbal form.**