**Secure Program Development**

Secure program development assures that there will be no data breaches at the business. To have a safe programming environment, security should be included in every part of the process. The software must meet certain security criteria as well as the project design's objectives. It begins with developing a system architecture that fits all of the criteria defined throughout the requirements process and then dividing the software into systems and subsystems, identifying their needs as well. Furthermore, the coding process for each component has a substantial influence on security. Finally, it passes through the testing process, where we look for unusual behaviors that might lead to security vulnerabilities. I would like to refer to the agile application development model, as it can be dynamic and flexible and also provides great maintenance for projects.

A method for testing and maintaining quality control is code review or peer review. It can be used for any type of deliverable software, design, or document. As a best practice, approaches such as formal code reviews, team reviews, walkthroughs, pair programming, peer desk checks, and pass-around must be used to discover strengths, flaws, and relative costs. Because the program is classified as restricted data under DoD CUI Information (800-171), all changes to it must go through appropriate code inspection. It is also a proven and effective way for improving quality, increasing security, reducing time to market, lowering maintenance expenses on the completed product, and reducing testing and rework time. Code review also helps reviewers learn new approaches, helps programmers generate better quality work, reduces bugs, and simplifies code maintenance.