

System Security Process Guide (a.k.a Security SLC)

Task Overview

SFA historically has used an SDLC that did not adequately address system security controls to be employed during the creation and deployment of its systems. Recently, the SFA security office developed an initial draft of a lifecycle checklist with critical security-related actions and deliverables identified to address this deficiency. The SFA security office asked KPMG Consulting to expand upon this effort and really think through the intricacies of the SDLC. Our initial goal was to identify, categorize and place every security requirement we determined to be a critical part of a system's lifecycle into one of the six system development lifecycle phases. During the second phase of the task order, we increased the intensity of our effort and reached out to the SDLC community to begin the socialization of our System Security Process Guide.

Task Description

Our approach to this task was to incorporate the draft SDLC checklist into guidance extracted from the NIST Self-Assessment questionnaire. We began the task by listing as many security-related tasks/documents that needed to be performed/created during a system's lifecycle as we could. From this list we organized the security requirements into categories of activities. For example, a major category heading was personnel security. Personnel security encompasses numerous tasks and deliverables that should be performed during various phases of a system's lifecycle.

To create the checklist we initially mapped each major category heading through the system lifecycle. Each category consists of numerous deliverables, which in turn are supported by several actions. These actions are completed by the SSO (Government staff) or the contractor support staff. If the contractor support staff are responsible for an action, it is the responsibility of the SSO to ensure that the action is completed, documented and delivered by the contractor to the SSO. Each deliverable is documented in a formal correspondence (see attached) at the completion of each phase. The checklist is signed and dated by the SSO and System Manager, thus completing the security requirements for the system lifecycle phase.

Once we were comfortable with our Security Lifecycle, we arranged to meet with the SLC working group within eCAD. The SLC working group immediately embraced our effort and encouraged our team to incorporate the security guidance into their SLC process guide. The final result of the security guidance incorporation effort was two-fold. The eCAD working group, along with direct assistance from our team, extracted language from our security guidance and inserted the text into the SLC. Second, we created a stand alone System Security Process Guide to assist those project members who are solely focused on the security components of the SLC. The System Security Process Guide includes several attachments to aid in the implementation of the process guide.

Task Status

Beginning the week of October 1, 2001, the System Security Process Guide will be introduced to the Modernization Partner Leadership. This briefing will kick off the extensive training effort with SFA and the Modernization Partner to begin the formal incorporation of security into SFA's solution lifecycle.