# Secure Acquisition
# Case 1: Acquisition/SCRM Project Initiation

**January 2020**

The purpose of secure SCRM is to identify and mitigate any risks in the software supply chain.

**Case Background**

WBYT has contracted with Detroit Defense to upgrade the F-16F aircraft. Specifically, Detroit Defense wishes to update the navigation system with Advanced Global Positioning System (GPS) capability that will allow that fighter-bomber to pinpoint targets down to the foot, even in overcast and nighttime conditions. The GPS model chosen for this aircraft has been used in a similar application for the fire control system for the AH64D Apache Longbow helicopter, so it is considered to be off-the-shelf (COTS). However, because it's a military item, modifications to the software will be required in order to integrate this GPS system into Detroit Defense aircraft. Revisions will need to be written (and/ or modified) to support the following needs:

a) *Integrate the GPS into the existing on board navigation system.*
b) *Display updated navigation information on the pilot's Head-Up Display (HUD).*
c) *Allow the pilot access to the modified navigation data through the Control Display Unit (CDU).*
d) *Communicate GPS information to ground control and to other aircraft in a mission. (Note: no equipment upgrades are planned to support the increased communications requirements.)*

In the case of the GPS/CDU Upgrade itself, the products are the onboard GPS Interface and the pilot CDU. This project can also be decomposed into the constituent management processes. In this case the major processes are project management, COTS acquisition and integration, COTS interface and software assurance support, software customization and risk management, supplier and software qualification, and post-development support.

In the case of the GPS Interface, the requirements are well known. The current navigation system and interface software is written in Java, and due to the limited nature of the changes to the navigation software, no change in language will be required. ISO 12207-2008 will be used as the software development and documentation standard for this acquisition. NIST 800-30 and NISTIR 7622 will be used to manage the risk portions and can be downloaded from the NIST publications website. ISO 15408 might also be consulted to describe any product certification needs. The final product will also have to satisfy all relevant elements of NIST 800-53

The contractor that developed the GPS system for the military will make the GPS software modifications on a subcontract to WBYT. Consequently, their supply chain will have to be vetted along with that of WBYT. WBYT will provide a specification of the modification requirements to all subcontractors however any subsequent product and process assurance up

and down the supply chain will be up to the individual subcontractors by contract. This will reduce the cost associated with modifying this aspect of the system.

WBYT has determined that besides any COTS acquisitions about 9,000 SLOC will have to be developed and/or modified to implement this new capability. The condition of the existing navigation software is not known, and the customer wants formal documentation, so it was assumed in the planning for the bid that the relative level of productivity would be at about the same level as that for a new development. Detroit Defense (acquirer) has contracted to supply a System/Subsystem Specification (SSS), a System Design Description (SSDD), and an Operational Concept Document (OCD). The acquirer will modify the OCD during development to reflect the changing needs of the system. WBYT will be responsible for the following technical documentation:

a) *Software and Interface Requirements Specifications (SRS & IRS)*
b) *Software and Interface Design Descriptions (SDD & IDD)*
c) *Software Assurance Case*
d) *Software Test Plan (STP)*
e) *Software Test Description (STD)*
f) *Software Test Report (STR)*
g) *System Qualification Test Report (SQTP)*
h) *Assurance Case Management Plan (ACMP)*

The developer will also be responsible for the following management and support documentation:

a) *Software Acquisition Plan*
b) *Software Assurance Plan*
c) *Software Risk Management Plan*
d) *Software Development Plan*
e) *Software Configuration Management Plan (SCMP)*
f) *Software Integration Plan*
g) *Software Qualification and Testing Plan (SQTP)*
h) *Software Transition Plan (STP)*
i) *A Software Version Description (SVD)*

**Prepare a Response to the Following Items**

For this first exercise you will define the potential functions required as well as who will supply them. You will take the following steps:

1. Identify a process in the case that you intend to support by a software application – this should include a scope, business case and assurance case statement
2. Define top-level functions required to carry out the desired process – these must be coherent (e.g., logically related and complete)
3. Decompose the top-level functions into a second level of component functions
4. Decompose the second level functions into a third level of component functions (e.g., formulate a component tree)
5. Assign a (imaginary) supplier for each component at all tiers – these will be assumed to be subcontracted relationships (e.g., the work will be done by a subcontractor directly employed by the higher-level entity)