# Secure Acquisition Case Study 3: Adequacy of Acquisition Practice

Dan Shoemaker, University of Detroit Mercy

**April 2021**

# Secure Acquisition Case Study 3: Adequacy of Acquisition Practice

## Background

Systems are built out of components that are integrated from the lowest level of a supply chain up to a finished product. This creates a serious weakness in that malicious code, or counterfeit parts can be inserted at the bottom of the process without scrutiny and then integrated up into the end-product, as was demonstrated by the recent SolarWinds hack.

The possibility of such a thing occurring is so obvious that you would think that there have been practical efforts to address it. However, even though we've expended much time and effort to ensure robust, efficient and defect free code, we have done very little to ensure against compromises that could occur during the integration process. Thus, the aim of this project is to help the student understand the stages involved in establishing supply chain capability, as well as present a sample solution.

## Case Study Overview

The purpose of this assignment is to evaluate the current capability maturity of your ICT supply acquisition security practice. The assessment will determine areas in your organization where proper acquisition risk management is being practiced, as well as the relative maturity of those practices. The goal is to generate a nominal ranking of capability maturity based on a universal scale of process performance.

The total set of potential practices in the recommendations of NIST 800-161 "Supply Chain Risk Management Practices for Federal Information Systems" is the most authoritative current reference for proper ICT supply chain risk management practice. The practices in NIST 800-161 apply differently within three different communities of practice: Acquirers, Suppliers, and Integrators. Therefore, depending on the role your organization plays you may be required to fill out this assessment tool for more than one community of practice. And as a consequence, three different assessment tools have been provided representing each of those notional communities.

## Student Instructions

Using the Case, please address each practice in the instrument (provided) as an individual, unique requirement. Provide your best estimate of the level of execution for each of these requirements. Depending on your judgment place a [number] "1" in the column that most appropriately describes the level of execution of each of the individual practices.

At the bottom of the instrument you will find a grand-total ranking for the degree of process capability for each of the columns. That sum is the total number of responses for each maturity level. You will be able to roughly determine your organization's level of capability maturity based on where the bulk of your responses fall. This will allow you to judge the relative maturity of your overall supply chain risk management process, as well as the areas where some improvement may be required.

## Instructor notes

This is an individual assignment done during a live-lab session. The process steps are taken a step at a time as guided by the instructor. This is done in-class as a first of four lab projects done over the semester to illustrate an explicit process for risk mitigation in supply chains using NIST 800-161 (see supplemental evaluation form)

## Example solution

For this case we are addressing the United States Air Force's need to upgrade F-16F aircraft. Specifically, as it pertains to updating the current navigation system with an Advanced Global Positioning System (GPS) capability. For this effort the GPS model chosen for this aircraft has been previously utilized in a similar application for the fire control system for the United States Army's AH64D (Apache Longbow helicopter). Consequently, it is considered to be a Commercial off the Shelf (COTS) application.

**Capability Maturity Assessment Tool - Supplier Community of Practice Summary**

| | | Not Done | Performed | Managed | Predictable | Optimized |
|---|---|---|---|---|---|---|
| I. | Contractor Name: Wild Blue Yonder Technologies Inc (WYBT)<br>Role: Prime Contractor: Updating Current Navigation System with GPS Capability | 3 | 63 | 96 | 0 | 0 |
| II. | Contractor Name: United States Army<br>Role: Sub-Contractor: Updating Current Navigation System with GPS Capability | 1 | 58 | 102 | 0 | 0 |
| III. | Contractor Name: United States Air Force<br>Role: Sub-Contractor: Updating Current Navigation System with GPS Capability | 3 | 53 | 106 | 0 | 0 |
| IV. | Contractor Name: Interlock Technologies, Inc. (8 (A) Contractor)<br>Role: Sub-Contractor: Updating Current Navigation System with GPS Capability | 8 | 70 | 84 | 0 | 0 |
| V. | Contractor Name: National Aeronautics and Space Administration<br>Role: Sub-Contractor: Updating Current Navigation System with GPS Capability | 2 | 56 | 104 | 0 | 0 |

Based on the examination and analysis of the summary results using the *Capability Maturity Assessment* tool for suppliers, we identified a concern with one of the sub-contractors identified for this effort (Interlock Technologies, Inc.) The concern relates to the sub-contractor's limited maturity in terms of the number of performance metrics that are not rated as optimized. While this concern exists, the fact that the sub-contractor is an 8 (A) Contractor, with preference provided by the U.S. Government. The Prime Contractor will implement additional contract surveillance controls to ensure that all work efforts performed under the contract along with any respective contract modifications will be met and at a level consistent with the performance requirements established for the work effort.

## References

Sigler, Ken, Dan Shoemaker and, Anne Kohnke, Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product, Auerbach Publications; (Internal Audit and IT Audit) 1st Edition, November 3, 2017

Shoemaker, Dan, and Kenneth Sigler, "Cybersecurity: Engineering a More Secure IT Organization", Cengage Learning, 2014, Chapters 5 and 7
ISO 27001 and ISO 27002 (provided as BS7799)

IEEE 1028-1997 Standard for Software Reviews

ISO/IEC 9126 – 1991 Software Product Evaluation - Quality Characteristics and Guidelines for Their Use (can be read as ISO/IEC 9126- 96)

IEEE 610 - Standard Glossary of Software Engineering Terminology

The Common Weakness Enumeration http://cwe.mitre.org/

Foreign Ownership, Influence or Control Investigations (FOCI)
http://www.dss.mil/isp/foci/foci_info.html