



SSCA Summer Working Groups 2015

Acquisition WG – EO 13636 Section 8e, Improving Cybersecurity And Resilience through Acquisition OEM Working Group and building a FAR Business Case

“Include a Requirement to Purchase from Original Equipment Manufacturers, Their Authorized Resellers, or Other “Trusted” Sources, Whenever Available, in Appropriate Acquisitions.”

- *In certain circumstances, the risk of receiving inauthentic or otherwise nonconforming items is best mitigated by obtaining required items only from OMs, their authorized resellers, or other trusted sources.*
- *The threshold for application of this risk mitigation should be consistent across the Federal government.*



Why OM/Authorized/"Trusted" Sources?

- Ensuring that the goods provided to the government are authentic and have not been altered or tampered with is an important step in mitigating risk.
- Inauthentic end items and components often do not have the latest security-related updates or are not built to the original equipment (or component) manufacturer's security standards.
- OMs have a heightened interest in ensuring the authenticity of their products, and this interest carries through into their policies for designating certain suppliers or resellers as "authorized."



Conflict with Socioeconomic Preferences and Competition Requirements?

- Limiting purchases to only these types of sources for *all* acquisitions may not be compatible with acquisition rules, socioeconomic procurement preferences, or principles of open competition.

So....

- Application of this requirement will be relatively narrow.
- Used only in cases where the mitigation provided by the use of OM/authorized/“trusted” source is appropriate to the risk of the purchase.

- Even with use of “trusted” sources, it may be possible to have “authentic” equipment that still has cyber vulnerabilities.
- This approach should only be used for purchases that present risks great enough to justify the negative impact on competition or price differences between “trusted” and “un-trusted” sources.
- For acquisitions that present these types of risks, this qualification should be incorporated into the full acquisition and sustainment lifecycles, starting with requirements definition, acquisition planning, and market research.

- Additional “trusted” sources can be identified through the use of qualified products, bidders, or manufacturers lists (QBL)(FAR 9.203).
- Using a QBL will help ensure:
 1. Definition of “trusted” supplier is transparent;
 2. Attainment of “trusted” status is not limited to companies that have obtained “authorized” relationship with an OM; and
 3. Identified sources meet appropriate standards for providing authentic items.



Steps Toward Requiring OEM and Authorized Sources

- **DoD-GSA Report: OEM/Authorized and other “trusted sources.” How to establish “other trusted sources?”**
 - First consider total cost – cost of acquisition of legacy equipment vs cost of system upgrade
 - 2nd – OEM awareness and liability waiver (DFARS/Sec 818/817)
 - 3rd – high-level approval of action (HCA, PEO, Agency, Congress??)
- **What are industry “best practices” for designating authorized resellers and how a potential reseller goes about becoming one...including of course, small businesses and other enterprises. This may also consider audit and enforcement best practices for those that violate terms and conditions of agreement.**
 - Definitions and associated requirements vary considerably, depending on the industry, products or service and many other factors.
 - Most often, term “authorized” indicates that some form of contractual and legally enforceable relationship is in place between the producer and seller of a good or service.
 - May also include strict requirements regarding a seller/reseller operations, financial stability, adherence to industry standards and other requirements, including auditing and other enforcement provisions to ensure compliance.



Steps Toward Requiring OEM and Authorized Sources (cont'd)

- **Require suppliers or resellers to adhere to commercial standards relevant to supply chain security (e.g., ISO, etc.)? What are the specific standards used? What standards have been used in the past or are being considered (i.e. ISO 27036, O-TTPS, SAE, NIST etc.)?**
 - Open Trusted Technology Provider Standard™ (O-TTPS)
 - ISO/IEC Information technology -- Security techniques -- Information security for supplier relationships
 - SAE Aerospace AS5553, Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition
 - C-TPAT, NIST SP 800-161,.....
- **How do we educate the U.S. Government acquisition / procurement professionals on how OEM's identity, select, vet, monitor, and inspect suppliers to achieve trust, authenticity, traceability, etc.?**
 - Acquisition from an authorized channel or business partner is a good starting point for establishment of trust.
 - How can the government determine how the authorized supplier manages their engineering / development processes to ensure the integrity of their supply chain.
 - No one method or indicator is solely capable of validating a trustworthy supplier.

- Explicitly define “trust” for purposes of QBL
 - Based on commercial best practices
 - Objective, measurable, relevant to security
- Develop FAR Business case:
 - PROPOSAL:
 - PROPOSAL DESCRIPTION:
 - AFFECTED PART/SUBPART: [PART OR SUBPART OF THE FAR]
 - BACKGROUND:
 - RATIONALE FOR THE CHANGE/VALUE/BENEFIT: [TO INCLUDE STATUTORY BASIS, POLICY BASIS, ETC., FOR THE CHANGE]
 - STAKEHOLDER POSITIONS IF KNOWN:
 - RECOMMENDATION AS WHERE THE SUGGESTED CHANGE SHOULD BE INCLUDED IN THE FAR, IF KNOWN:
 - RECOMMENDED FAR TEAM, IF KNOWN [LAW TEAM, IT TEAM, ACQUISITION STRATEGY TEAM, SMALL BUSINESS TEAM, FINANCE TEAM, IMPLEMENTATION TEAM].
 - PROPOSAL SPONSOR AND POC FOR ADDITIONAL INFORMATION ABOUT THIS REQUEST. [INCLUDE NAME, TITLE, E-MAIL AND TELEPHONE NUMBERS]
 - PROPOSED REVISIONS TO THE FAR (ATTACH SPECIFIC PROPOSED REVISIONS TO THE FAR TO INCLUDE DELETED AND ADDITIONAL LANGUAGE)