



Written Testimony, Aerospace Industries Association, June 16, 2014

Subject: “Public Meeting, Detection and Avoidance of Counterfeit Electronic Parts – Further Implementation”

Presented By: Rusty Rentsch
Assistant Vice President, Technical Operations
rusty.rentsch@aia-aerospace.org
(703) 358-1054

The Aerospace Industries Association (AIA) welcomes the opportunity to provide further input and requests for clarification regarding further implementation of “Detection and Avoidance of Counterfeit Electronic Parts”. AIA was founded in 1919 and is the premier U.S.-based trade association representing more than 350 major aerospace and defense manufacturers and suppliers and approximately 844,000 aerospace and defense workers. Our members represent the leading manufacturers and suppliers of civil, military and business aircraft, helicopters, unmanned aircraft systems, missiles, space systems, aircraft engines, materiel and related components, equipment services and information technology.

AIA’s consensus evaluation of the recently released rule indicates there are several areas for which the aerospace industry is seeking clarification. It is mutually beneficial to have a common understanding between industry and the customer community regarding its implementation. In some cases, varying interpretations of elements of the rule could drive significant infrastructure changes within industry. Thus, AIA seeks to obtain clarification and offer industry perspective as to these interpretations and their impacts below:

1. Inventory – in the commentary to the recently released DFARS rule, it states:

“Parts already on the shelf

Comment: A respondent asked how the rules would be applied to parts that had been purchased already and were on the shelf.

Response: If the parts are already on the contractor’s shelf or in inventory, and they were not procured in connection with a previous DoD contract, they will be subject to the same requirements, such as traceability and authentication.”

- a. Industry requests further clarification of this comment as it appears to place an undue, additional burden on those suppliers, product lines that are not “one off” for government use, but instead rely on “pool buys” and “pool builds” to support government contracts. In these cases, parts are often procured in inventory not specific to a particular contract. However, the ultimate destination would be a US government contract. Additionally, this places an undue burden on Commercial Off-The-Shelf (COTS)/ commercial suppliers who have already demonstrated their unwillingness to accept provisions beyond their standard warranties. It is impractical to consider they will purge inventory prior to providing parts to US government contracts if this is what is implied in the commentary preceding the DFARS rule. If so, it is industry’s interpretation that contractors will have to perform additional traceability verification and/ or authentication screening of COTS/ commercial items and those costs would be considered allowable. Please clarify.

- b. Comingled inventories and grouped purchases are common procurement and inventory management practices. These practices are employed to help manage costs on government programs. How will this apply to contractors that use comingled inventory for the types of parts in consideration and do not peg inventory for specific programs and contracts? This provision is likely impractical and unenforceable in these circumstances. The processes needed to meet the expectations outlined in the DFARS could require a strict allocation approach and segregated inventories by program. Such approaches would increase costs to the government if implementable at all throughout the supply chain.
 - c. What specifically are the requirements for traceability and authentication that the on-the-shelf inventory will be subject to?
 - d. Industry requests clarification on whether an exception will exist. Is the fact that inventory was procured in connection with a DoD contract an exception to the requirements? If inventory was not procured exclusively for a DoD contract, but instead purchased for use in multiple applications including DoD contracts, are these “parts already on the shelf” exempt from the requirements of the rule? What if the parts were not procured in connection with a previous DoD contract, but were procured for another Government end-use? Do such parts qualify for the exception?
2. **Supplier governance and purchasing system approvals** – Industry requests further clarification as to how the government intends to implement the oversight provisions of this rule as it applies to Contractor Purchasing System Reviews (CPSR) approvals. Given the significant liability imposed on contractors, it is likely that contractors will continue, or likely increase, their duplicative oversight of the supply base related to counterfeit mitigation. This is in addition to the planned/ongoing oversight on the part of Defense Contract Management Agency (DCMA) and other government agencies. Such duplicative oversight is considered an allowable expense, and impactful to the affordability of systems provided to the government. Could the government consider providing a process/schedule for implementation of supply base oversight? This would allow contractors to plan their oversight accordingly.
- a. As DCMA develops their processes/ instructions for inclusion of counterfeit detection and avoidance systems into their CPSR instructions, industry offers to partner with DCMA in this process. This would ensure such instructions are understood by the contractors being reviewed and would eliminate inefficiencies in the oversight process. Industry has been addressing counterfeit detection processes and standards for several years and has input that could benefit government and industry as such oversight is formulated.
 - b. Would the government consider providing “safe harbor” if a contractor utilizes a supplier whose purchasing/counterfeit avoidance system has been approved by DCMA?
 - c. Would the government consider providing a “safe harbor” if contractors utilize a supplier whose counterfeit avoidance system has been reviewed and approved by a 3rd party? Such a 3rd party review process (similar to AS9100 certifications) could be subjected to DCMA oversight. Provision of safe harbor in these circumstances would alleviate contractors (and in particular suppliers at lower tiers of the supply chain) the unnecessary burden of duplicative oversight.

3. **Availability of electronic parts and associated governance process** – the DFARS instructs, *“Use of suppliers that are the original manufacturer, sources with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources.”*
 - a. On occasion, electronic parts are not available from these sources. “Availability” can be influenced by factors such as: obsolescence, schedule (i.e. supporting a critical operational need in theatre) and minimum buys from an Original Equipment Manufacturer (OEM) or authorized source. Is it the government’s intent to provide further guidance for these circumstances? What is the associated governance practice contemplated? For example, must the Procuring Contracting Officer (PCO) or Administrative Contracting Officer (ACO) direct procurement from an alternate source in these instances? Will that provide risk relief to contractors? Will the Defense Logistics Agency (DLA) supply parts in these circumstances and if so, will DLA supplied parts be considered under the safe harbor rules as Government Furnished Equipment (GFE)?
4. **Commercial items** – Is there intended to be a waiver process for COTS and commercial items? It is anticipated that many provisions of this DFARS will not be accepted by such suppliers who tend to provide their standard terms and warranties. What is the government’s intended approach for its own procurements?
5. **Extension to embedded software and firmware** – How does this relate to the government’s intended oversight of “supplier risk” and the provisions of DFARS Clause 252.204.7012, "Safeguarding Unclassified Technical Information" (issued Nov '13)? Industry recognizes that embedded software and firmware represents a risk in certain electronic parts and assemblies that contain electronic parts. Industry requests additional information regarding the expectations and scope related to counterfeit detection and prevention with regard to embedded software and firmware. The detection of the electronic hardware portion of electronic parts is very different from the software and firmware portion of the same potential devices. Clarification of expectations from the government could help reduce costs associated with testing and verification of embedded software and firmware. How is “intent” proven? How is inspection and test to be performed? What is the government’s intended approach for its own procurements?
6. **Traceability documentation requirements & verification** - Industry seeks clarification of the DFARS as it relates to traceability, as there could be varying interpretations with widely different impacts. Typical traceability processes employed generally by industry may not meet some DFARS expectations, and there could be considerable cost/ feasibility implications depending on the specific interpretation of DFARS “traceability” requirements. Specific areas of concern include:
 - Current industry processes generally do not include the name and location of all of the supply chain intermediaries between the part manufacturer and the seller. Commercial suppliers have already demonstrated their unwillingness to accept provisions beyond their standard practices because of low volume revenue streams the aerospace and defense industry provides the electronic components industry.
 - Documentation is limited to procurement history versus Certificate of Compliance’s or other documentation.
 - Parts received in stores are typically co-mingled after inspection and are considered acceptable for use without any further tracking/ consideration (space / nuclear applications may be the exceptions, with additional traceability, albeit at significant cost). Thus specific traceability from component to end item is not a standard practice within industry.

The language within the DFARS regarding traceability implies the expectation to have traceability information for electronic parts and assemblies which contain electronic parts procured from “non-authorized” sources. This includes Commercial items and COTS. Industry would like confirmation on the interpretation of this rule as follows:

- 1) Electronic parts or assemblies that contain electronic parts from authorized sources do not require internal traceability by contractors. Instead, contractors should rely on the existing processes of those authorized sources.
- 2) Further, the DFARS appears to imply that electronic parts or assemblies that contain electronic parts from “non-authorized sources” will require the full chain of custody /traceability outlined in the DFARS. If the interpretation outline above is correct, particularly as it applies to item #2, industry would like to highlight the following significant impact/ questions:
 - Is it correct to interpret that in cases where this traceability is not available during the procurement process but the procurement is required to support government contracts, the contractor may apply a risk based approach, including authentication testing in order to procure the parts? Further, would the execution of this logic be subject to review and approval under the CPSR?
 - If traceability is required for such any electronic parts in completed assemblies delivered to the government, that significant changes to inventory and manufacturing processes will result in many circumstances. These revisions will drive significant cost growth for DoD programs. As described in chart 1 below, common practice in industry is to maintain traceability up through receipt/ inspection, at which time parts are placed in secured inventory with other parts and such traceability is not maintained. This change affects inventory and manufacturing practices throughout industry if the above interpretation reflects DoD’s intent. Industry recommends that the traceability requirement be limited to procurement history records to authorized sources and that traceability requirements end upon receipt in stores.
 - If industry receives parts or assemblies as GFE from DLA or other government agencies, will such traceability be provided for authorized and non-authorized sources?
 - Acceptance of such provisions with commercial/ COTS suppliers is unlikely. Will there be a waiver process in these circumstances?

Typical Traceability Processes

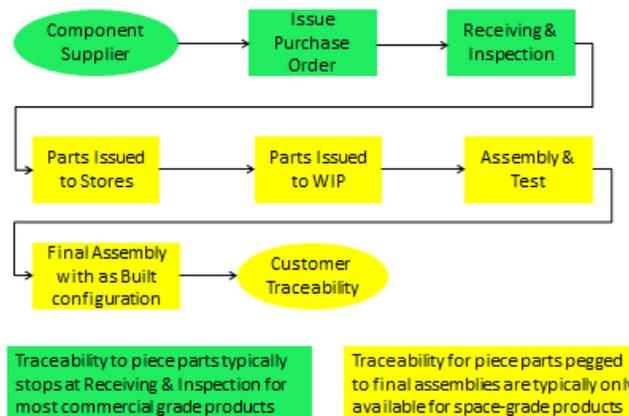


Chart 1 – Typical traceability/ inventory practices employed by industry



7. **Small Business impact verification** - Could the government provide clarification/ guidance for industry as to how to address the inevitable situation that will occur when Non-Cost Accounting Standards (CAS) covered suppliers reject flow down of these requirements? Is it contemplated that waivers will be required in each of these circumstances? How will these circumstances impact CPSR approvals for the buying contractor? The process developed to address this should consider the likely rejection of these requirements by many COTS and commercial suppliers, who, as a matter of practice, provide standard warranties for commercial products but tend to reject further flow down of requirements such as these.

8. **Additional Clarifications** - The following provisions of the rule require further clarification as to the government's intent and planned oversight. These must clearly be accomplished in partnership with the government:
 - a. Processes to abolish counterfeit parts proliferation.
 - b. Design operation and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.
 - c. Control of obsolete electronic parts. Industry requests clarification of the government's role in this process (i.e. funding, redesigns, etc).
 - d. Reporting and Quarantining:
 - i. DFARS 252.246-7007(c)(6) prescribes reporting requirements for when the Contractor knows or suspects that any electronic part purchased by or for the DoD is counterfeit or suspect counterfeit. Due the rule's flow-down requirement, the prime contractor, its subcontractors, and any service organization (e.g. a test laboratory) all have requirements to report and quarantine the parts. Which of these is the party intended to report and quarantine? Is it the party with title to the material, or the prime contractor if the subcontractor holding title does not submit a GIDEP within a reasonable period of time (which is in alignment with industry standards, AS6081)?
 - e. Clarification of the timing and triggers to determine unallowable costs associated with remedying a counterfeit electronic part escape is requested by industry. Industry assumes costs to prevent counterfeit parts proliferation are allowable as has been standard practice.

AIA and their industry members would like to continue the dialog with the government to understand the reconciliation/ alignment of this rule with other proposed/ contemplated rules in this arena. For example, AIA desires for alignment between FAR Case 2012-032 "Higher Quality Requirements" AS5553 with DFAR 252-246-7007, and notifications with FAR Case 2013-002. If you have any questions or require further information, please contact me by telephone at (703) 358-1054 or by e-mail at: rusty.rentsch@aia-aerospace.org.

Sincerely,

A handwritten signature in black ink, appearing to read 'James R. Rentsch', is written over a light blue background.

James R. Rentsch
Assistant Vice President, Technical Operations