'Contractor Counterfeit Electronic Part Detection and Avoidance Systems' and Compliance with DFARS Clause 252.246-7007

By Henry Livingston

DoD published an amendment to the DFARS requiring "covered contractors" to establish and maintain an acceptable "Counterfeit Electronic Part Detection and Avoidance System"[1] and to flow down the substance of system requirements in subcontracts. The DFARS 252.246–7007 applies the central tenets recommended by industry and US Government subject matter experts:

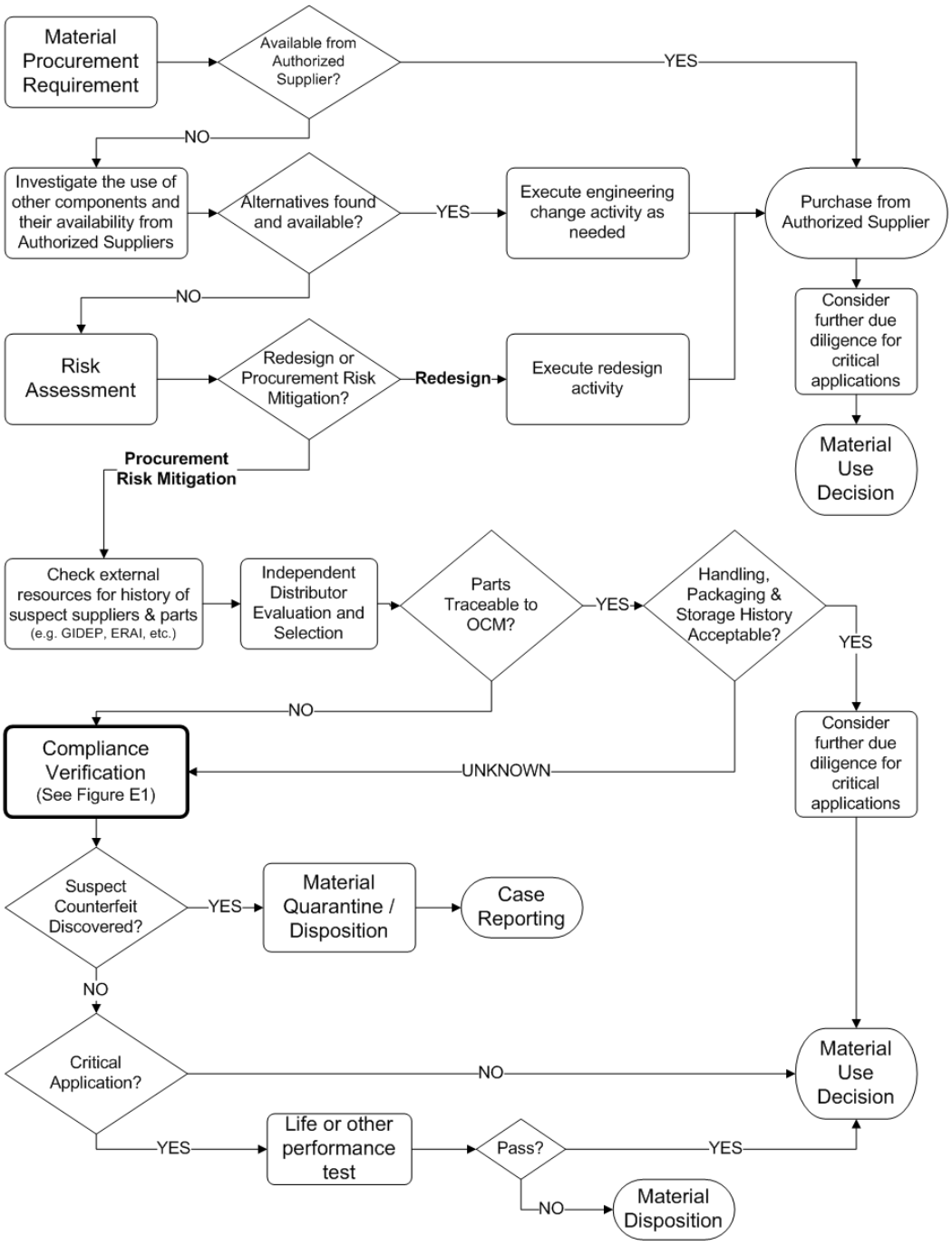
- Obtain electronic parts, whenever possible, from original manufacturers or their authorized distributors
- Perform due diligence when purchases from sources of supply other than the original manufacturer and its authorized distribution chain are necessary
- Notify government and industry of suspected counterfeits when they are encountered

A "Counterfeit Electronic Part Detection and Avoidance System" described in DFARS 252.246–7007 must include risk-based policies and procedures that address the following elements:

1. The training of personnel.
2. The inspection and testing of electronic parts ….
3. Processes to abolish counterfeit parts proliferation.
4. Processes for maintaining electronic part traceability….
5. Use of suppliers that are the original manufacturer, or [an authorized supplier] ….
6. Reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts ….
7. Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit ….
8. Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts ....
9. Flowdown of counterfeit detection and avoidance requirements ….
10. Process for keeping continually informed of current counterfeiting information and trends ….
11. Process for screening GIDEP reports and other credible sources of counterfeiting information to avoid the purchase or use of counterfeit electronic parts.
12. Control of obsolete electronic parts ….

[1] Federal Register Vol. 79, No. 87 at p. 26108, 252.246–7007 Contractor Counterfeit Electronic Part Detection and Avoidance System

The following diagram presents an overview of a holistic counterfeit electronic parts avoidance and detection process and illustrates the interrelationship between key elements of an effective "Counterfeit Electronic Part Detection and Avoidance System". This diagram is taken from SAE Aerospace Standard AS5553, Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Revision A.[2]



[2] AS5553 Figure B3 - Procurement Risk Mitigation

DFARS Clause 252.246-7007 encourages the use of Government or industry recognized standards, such as AS5553, for the design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.[3] This paper offers guidance to contractors and subcontractors in establishing and implementing a "Counterfeit Electronic Part Detection and Avoidance System" that complies with DFARS Clause 252.246-7007; and describes how SAE Aerospace Standard AS5553 can be used to articulate requirements for a "Counterfeit Electronic Part Detection and Avoidance System" and to serve as criteria for assessing the adequacy the system.

[3] DFARS 252.246–7007 (c) (8) Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.

Personnel Training[4] and Keeping Current[5]

The contractor and subcontractor must train personnel in counterfeit electronic parts detection and avoidance. The training program should consist of general awareness training for a broad range of personnel, and more specialized and tailored training for personnel responsible to implement the organization's "Counterfeit Electronic Part Detection and Avoidance System".

Awareness training might include background information describing what counterfeit electronic parts are, their origins, how they enter the supply chain, vulnerabilities to counterfeit parts (e.g. obsolete and hard-to-find parts), new laws and regulations, and an overview of internal processes and methods to avoid and detect counterfeit electronic parts.

Specialized and tailored training would include supplier selection practices, procurement practices to avoid counterfeits, counterfeit detection implementation (through internal resources and/or 3rd party laboratory and analysis facilities), suspect counterfeit and counterfeit electronic part reporting practices, requirements flow down to suppliers, etc.

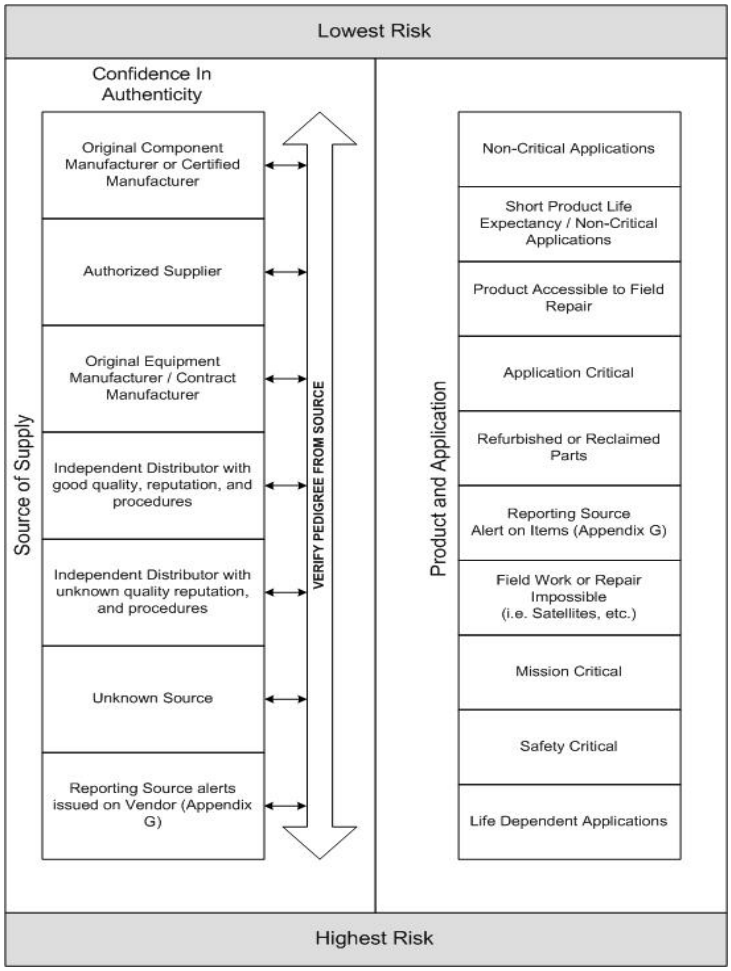
While a contractor and subcontractor may elect to establish its own training program (particularly for implementation of company specific policies and processes), a contractor or subcontractor could also take advantage of third party training programs, such as those deployed by SAE International concerning key industry standards, and the Government Industry Data Exchange Program concerning reporting practices. Various industry and government organizations conduct symposiums, seminars and conferences where related practices are discussed, such as the National Defense Industrial Association (NDIA), Aerospace Industries Association (AIA), American Bar Association (ABA), the Counterfeit Microelectronics Working Group host by the US Intellectual Property Rights Enforcement Center, the US DoD Defense Standardization Program Office, and many others.

Third party training programs, symposiums, seminars, conferences and other resources should be used to help keep personnel and internal processes up to date. These resources provide current counterfeiting information and trends, detection and avoidance techniques, industry standards, etc.

[4] DFARS 252.246–7007 (c) (1) The training of personnel.
[5] DFARS 252.246–7007 (c) (10) Process for keeping continually informed of current counterfeiting information and trends …

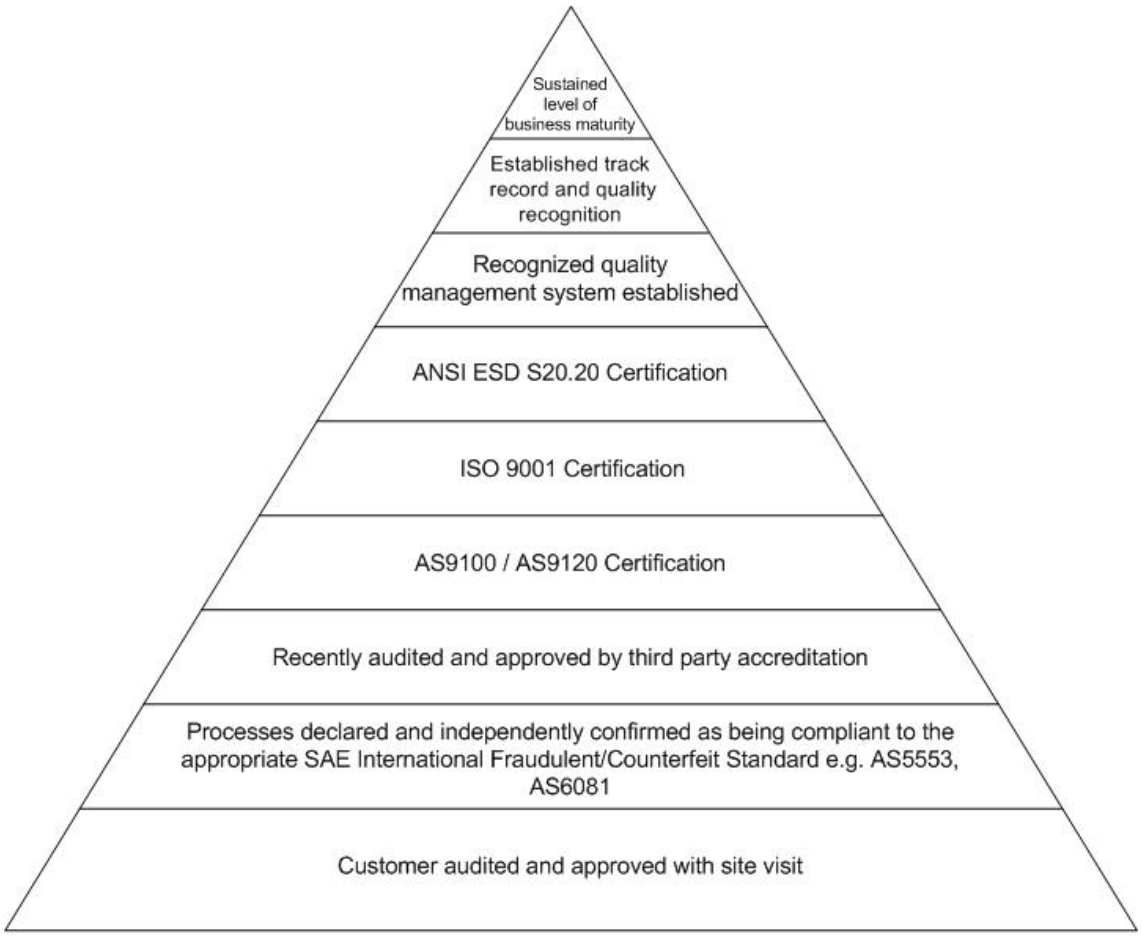
Supplier Selection[6]

The risk of purchasing counterfeit electronic parts is predominantly driven by the contractor's or subcontractor's use of suppliers. The most effective way to avoid counterfeit electronic parts is to acquire and use material from the Original Component Manufacturer (OCM) or the OCM's authorized distributor. Seeking out material from a supplier who plans to acquire material from, or possesses inventory acquired from other suppliers who are not the OCM's authorized distributors, should only be considered when compelling need precludes acquiring material from the OCM or the OCM's authorized distributor. The following diagram is taken from SAE International Standard AS5553[7] and presents a notional relationship between levels of risk, types of part suppliers within the supply chain and the criticality of the application where parts are to be used.



[6] DFARS 252.246–7007 (c) (5) Use of suppliers that are the original manufacturer…
[7] AS5553 Figure 4.2-1 - Risk Stack Chart

When selecting suppliers who are not the OCM or the OCM's authorized distributor, contractors and subcontractors should select suppliers that have been determined to be responsible and reliable sources through organization's established Procurement and Quality Assurance practices. The following diagram taken from AS5553[8] identifies factors for assessing and mitigating supplier risk.



Attempt to fill in more area within the pyramid for less risk

Standards activity is underway to document assessment criteria and to establish certification programs for a contractor and subcontractor electronic parts avoidance and detection processes.

When compelling need, such as obsolescence, precludes acquiring material from the OCM or the OCM's authorized distributor, documented protective measures must be implemented to avoid procurement and use of counterfeit electronic parts. The following section on inspections and tests, traceability, and other methods describes the particulars.

[8] AS5553 Figure 4.2-2 - Supplier Assessment Pyramid

The Role of Inspections and Tests[9] [10], Traceability[11] and Other Methods in Counterfeit Electronic Part Detection and Avoidance

The purchase and use of counterfeits can be avoided if one (a) acquires electronic parts from the original component manufacturer (OCM) or the OCM's authorized distributors, or (b) can confirm the hand offs of parts to the OCM or the OCM's authorized distributors. Some Independent Distributors acquire electronic parts from an OCM or the OCM's authorized distributors and can confirm these transactions. In the case of electronic parts acquired from the open market, however, suppliers generally cannot confirm traceability to the OCM or the OCM's authorized distributors. It is this inability to confirm traceability to the OCM or the OCM's authorized distributors that prompts the need to apply inspections, tests and other methods designed to avoid the procurement and use of counterfeits. This procurement risk mitigation process is described in SAE Aerospace Standard AS5553.[12] Taking a cue from government and industry subject matter experts, the US Congress included this expectation in the original legislation that initiated the final rule under DFARS Case 2012-D055.[13]

An organization meets the *traceability* requirements of AS5553 and the objective of DFARS 252.246–7007(c)(2) and (4) if the organization establishes and applies processes and procedures that …

> *(a) assure procurement from the OCM or the OCM's authorized distributors*
> The organization needs not seek out traceability (and associated artifacts mapping the path to the OCM) when it purchases parts from the OCM itself or when it purchases parts from the OCM's authorized distributors. The organization's procurement and receiving records confirming the organization's source should suffice.
>
> *(b) confirm traceability to the OCM for parts procured from other suppliers*
> If the organization uses a supplier to acquire material on the organization's behalf (such as an SDB to meet FAR requirements for small business set asides), that supplier needs to provide evidence that it acquired the material from the OCM itself or from the OCM's authorized distributors (e.g. the organization directs the sourcing to the OCM or the OCM's authorized distributors and the organization previously evaluated the supplier's ability to follow instructions). The organization's procurement and receiving records confirming its supplier's source should suffice.

[9] DFARS 252.246–7007 (c) (2) The inspection and testing of electronic parts…
[10] DFARS 252.246–7007 (c) (7) Methodologies to identify suspect counterfeit parts…
[11] DFARS 252.246–7007 (c) (4) Processes for maintaining electronic part traceability…
[12] AS5553 Appendix B – Purchasing Process, Figure B3 – Procurement Risk Mitigation.
[13] H.R.1540: National Defense Authorization Act for Fiscal Year 2012, Sec. 818. Detection and Avoidance of Counterfeit Electronic Parts

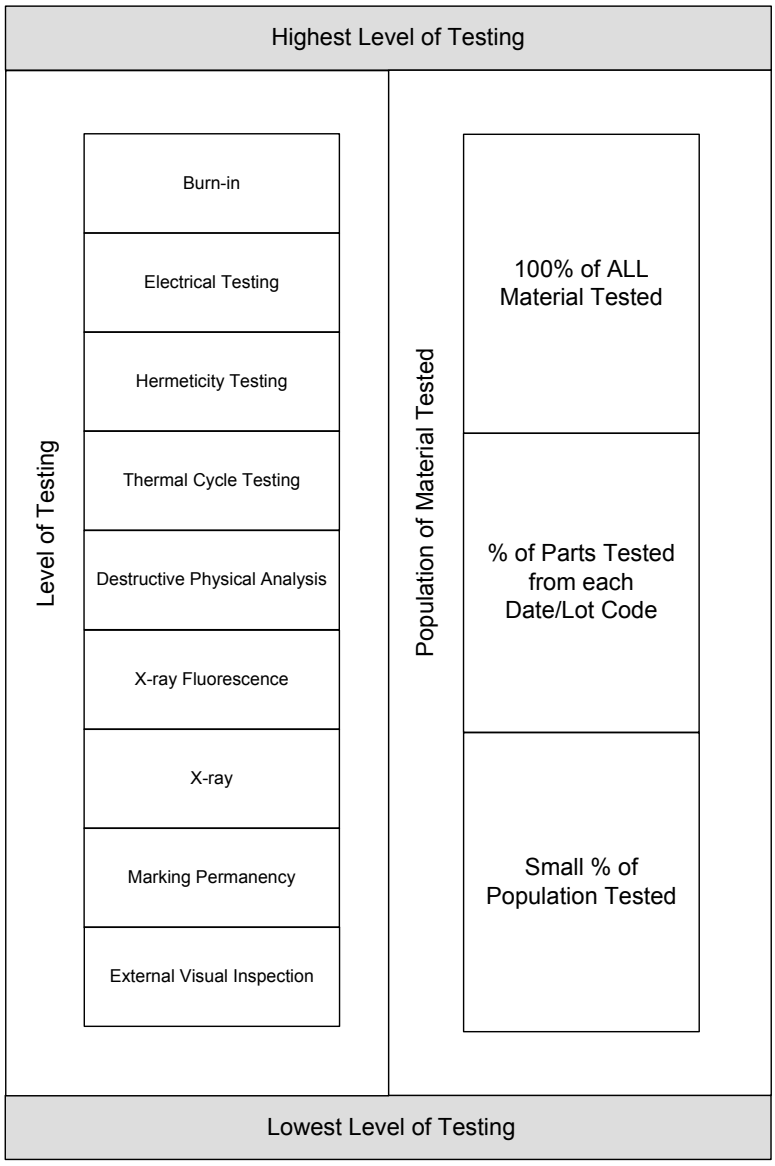
(c) apply inspections, tests and other methods designed to intercept and avoid the use of counterfeits when unable to confirm traceability to the OCM or the OCM's authorized distributors.
If the organization finds a compelling need to seek out material from a supplier who plans to acquire material from, or possesses inventory acquired from other suppliers who are not the OCM or the OCM's authorized distributors (e.g. purported 'authentic OEM surplus', part sourced from the open market, etc.), the organization should seek out and evaluate the integrity of supply chain traceability information mapping the path to the OCM (e.g. contact the intermediaries and OCM to verify the evidence provided is associated with the parts supplied, etc.) and seek out information to verify adequate storage and handling. In the absence of verifiable traceability data and proof of adequate storage and handling, and in the absence of support from the OCM, the organization should see to the performance of tests and inspections designed to detect counterfeit electronic parts. The outcome of these tests and inspections should serve as the basis for "credible evidence" providing "reasonable doubt that the electronic part is authentic".

When selecting tests and inspections to detect counterfeits, DFARS 252.246–7007 calls for selection based on minimizing risk to the Government, [14] and requires that determination of risk shall be based on …

a. the assessed probability of receiving a counterfeit electronic part;
b. the probability that the inspection or test selected will detect a counterfeit electronic part; and
c. the potential negative consequences of a counterfeit electronic part being installed (e.g., human safety, mission success) where such consequences are made known to the Contractor.

The following diagram taken from AS5553[15] presents a notional relationship between the selection and application of tests and inspections to detection counterfeit electronic parts commensurate with product risk.

[14] DFARS 252.246–7007 (c) (2) The inspection and testing of electronic parts…
[15] AS5553 Figure 4.5-1- Test Evaluation Risk Stack Chart



Standards activity is underway to assist contractors and subcontractors in the selection inspections and tests to detect counterfeit parts, to describe the procedure for these inspections and test, and to define acceptance and rejection criteria for those inspections and tests.[16]

[16] Proposed AS6171, Test Methods Standard; General Requirements, Suspect/Counterfeit Electrical, Electronic, and Electromechanical Parts

Abolishing Counterfeit Electronic Parts Proliferation[17] through Reporting, Quarantining,[18] and Screening Reports from Credible Sources[19]

DFARS 252.246–7007 requires the reporting of counterfeit electronic parts and suspect counterfeit electronic part findings to Contracting Officer and to the Government-Industry Data Exchange Program (GIDEP). When counterfeit electronic parts and suspect counterfeit electronic part are encountered, these events should be promptly communicated both to Government and to industry. Sharing this information in a broadly accessible forum, such as the Government-Industry Data Exchange Program (GIDEP), enables other purchasers of the same or similar components to learn of this finding and be able to (a) examine their inventories and quarantine any questionable material they identify as well as (b) to check their open purchase orders to ascertain whether or not such components may be on order from the same or similar sources of supply.

Other regulations require reporting of possible violations of a contractor's code of business ethics and conduct.[20] The final rule under DFARS Case 2012-D055 notes that although DoD recognizes the importance of the "mandatory disclosure" rules, this may not be an appropriate use of them because it suggests a contractor has committed an "ethical or code of conduct violation." [21] DFARS 252.246–7007, standing alone, does not expand the reporting obligations of a Contractor beyond those currently articulated at FAR 52.203-13(b)(3)(i). FAR 52.203-13(b)(3)(i). The mandatory DoD IG reporting requirement of would not apply to the discovery of a counterfeit electronic part in the following circumstances:

- In those contracts issued before December 2008 where the subject FAR Clause was not subsequently incorporated;
- In those contracts with a dollar value of less than $5 million or with a performance period of less than 120 days;
- For contracts subject to FAR 52.203-13, in those situations where the Contractor has no creditable evidence that a subcontractor of the Contractor has committed a violation of federal criminal law involving fraud, conflict of interest, bribery, or gratuity violations found in Title 18 of the U.S. Code or a violation of the False Claims Act, 31 U.S.C. 3729-3733.

However, the contractor is still obliged to report the finding to GIDEP.

[17] DFARS 252.246–7007 (c) (3) Processes to abolish counterfeit parts proliferation.
[18] DFARS 252.246–7007 (c) (6) Reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts
[19] DFARS 252.246–7007 (c) (11) Process for screening GIDEP reports and other credible sources …
[20] e.g. FAR 52.203-13(b)(3)(i) and DFARS 203.1003(b)
[21] Federal Register Vol. 79, No. 87 at p. 261023, 10. Reporting

Contractors and subcontractors can play an important role toward abolishing counterfeit electronic parts proliferation by preventing their reintroduction into the supply chain. In the event a contractor discovers suspect counterfeit or counterfeit electronic parts in the course of materiel procurement, product inspection and testing activity, product failure analysis activity, etc.; the contractor must take steps to ensure the suspect counterfeit or counterfeit electronic parts do not find their way back into the supply chain. If counterfeit electronic parts are returned to the supplier, the parts could be resold to another user. Suspect counterfeit parts must not be returned to the supplier or otherwise returned to the supply chain until such time that the parts are determined to be authentic. AS5553 describes approaches to deal with counterfeit electronic parts.

Contractors and subcontractors should monitor GIDEP reports and other credible sources of counterfeiting information. These reports provide information to help avoid the purchase and use of counterfeits and suspect counterfeit parts discovered by others and to identifying suppliers associated with sales of these parts. These reports often include information about how specific suspect counterfeit electronic parts were discovered which can provide insights to help contractors and subcontractors canvass their inventories and open purchase orders as well as refine and improve their own counterfeit electronic parts detection and avoidance practices.

Obsolescence Management and Its Relationship to Counterfeit Electronic Part Avoidance[22]

Defense and aerospace products are particularly vulnerable to counterfeit parts due to part obsolescence. Microelectronics products, in particular, have life cycles far shorter than the defense / aerospace products that use them. When obsolete parts are not eliminated from product designs, suppliers other than the OCM or authorized distributors are often used to obtain components that are no longer in production. While changes to procurement practices will reduce the number of purchases from higher risk suppliers, the prominence of through-life support contracts will make part obsolescence a larger challenge and counterfeits a possibly bigger problem for DOD and defense contractors in the future.

In order to reduce the likelihood of having to purchase parts through riskier supply chains, contractors and subcontractors should apply obsolescence management practices to maximize the availability and use of authentic, originally designed, and qualified electronic parts throughout the product's life cycle. AS5553 includes guidance in this area and lists government and industry documents describing obsolescence management practices.

Customers are often constrained in their ability to support and fund approaches to eliminate the use of obsolete components. In these circumstances, contractors and subcontractors must (1) assure trustworthy sources of supply for obsolete electronic parts and, (2) when electronic parts must be acquired from other than the OCM or authorized distributors, apply inspections, tests and other methods designed to avoid the procurement and use of counterfeit electronic parts.

[22] DFARS 252.246–7007 (c) (12) Control of obsolete electronic parts …

Flowdown of Counterfeit Detection and Avoidance Requirements[23]

Contractors and subcontractors should include counterfeit detection and avoidance requirements in subcontracts and purchase orders. DFARS 252.246–7007 specifically requires the contractor to include the substance of the requirements for a "Contractor Counterfeit Electronic Part Detection and Avoidance System" in subcontracts. The expectation of DFARS 252.246–7007 is that counterfeit detection and avoidance requirements flow down at all levels in the supply chain that are responsible for buying or selling electronic parts or assemblies containing electronic parts, or for performing authentication testing.

Counterfeit avoidance and detection requirements should be context sensitive and relevant for the type of supplier and their role within the supply chain. For example, requirements directed to an upper tier subcontractor furnishing systems that contain electronic parts would differ from requirements directed to an electronic part distributor. In the case of an upper tier subcontractor, the flow down would include the substance of the requirements in DFARS 252.246–7007 that define a "Contractor Counterfeit Electronic Part Detection and Avoidance System". In the case of an electronic part distributor, appropriate requirements would be for the distributor to supply only product for which it is an authorized supplier or to supply products acquired from a supplier that is an authorized supplier. Counterfeit avoidance and detection requirements should include an expectation of the supplier to flow down the requirements to its suppliers.

[23] DFARS 252.246–7007 (c) (9) Flowdown of counterfeit detection and avoidance requirements …

Conclusion

In order to be responsive to DoD requirements for counterfeit electronic parts detection and avoidance, such as DFARS 252.246–7007, contractors and subcontractors must establish and maintain a holistic counterfeit electronic parts avoidance and detection process. SAE International Standard AS5553 can be used for the design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts that complies with DFARS 252.246–7007.