July 12, 2013

Defense Acquisition Regulations System
Attn: Ms. Meredith Murphy
OUSD (AT&L) DPAP/DARS
Room 3B855
3060 Defense Pentagon
Washington, DC 20301–3060

Subject: DFARS Case 2012-D055 Definitions

Dear Ms. Murphy:

The SAE G-19T Definitions Task Group fully supports the Congressional intent expressed in the FY12 National Defense Authorization Act (NDAA) (Pub. L. 112-81, Dec. 31, 2011) to avoid the introduction of counterfeit electronic parts and used parts sold as new into products sold to the Department of Defense. With the goal of collaborating with DoD to find solutions to counterfeit electronic parts issues, SAE is pleased to submit the following comments and recommendations regarding the proposed definitions published in DFARS Case 2012-D055.

SAE International is a global body of scientists, engineers, and practitioners that advances self-propelled vehicle and system knowledge in a neutral forum for the benefit of society. SAE was founded in 1905 and is comprised of over 130,000 vehicle engineers in 100 countries. SAE has a long history of coordinating with DoD and has published approximately 9000 technical standards, with more of them having been adopted for DoD use than those of any other organization.

In 2007, the SAE G-19 Counterfeit Electronic Components Committee was formed to address methods of preventing, detecting, responding to, and counteracting the threat of counterfeit electronic components through the development of standards suitable for use in aeronautic, space, defense, civil and commercial electronic equipment applications. These standards comprise global industry best practices in component management, supplier management, procurement, inspection, test/evaluation methods and response strategies to mitigate the proliferation of suspect or counterfeit components. The G-19T subcommittee has since been established to align the definitions associated with counterfeit parts prevention across the various G-19 subcommittees. Since DFARS Case 2012-D055’s publication, the G-19T task group has worked diligently to evaluate and suggest improvements for the definitions associated with the proposed regulations. The results of this effort are the following recommendations, which the committee is pleased to have the opportunity to provide.
Comments and Recommendations

Counterfeit Part –

DFARS Case 2012-D055 Current proposed definition:

Counterfeit part means—

(1) An unauthorized copy or substitute part that has been identified, marked, and/or altered by a source other than the part's legally authorized source and has been misrepresented to be from a legally authorized source;

(2) An item misrepresented to be an authorized item of the legally authorized source; or

(3) A new, used, outdated, or expired item from a legally authorized source that is misrepresented by any source to the end-user as meeting the performance requirements for the intended use.

As currently drafted, the definition contained in the proposed rule may encompass a greater variety of situations and products than was intended. To scope the term in better alignment with the Section 818 legislation, our first recommendation is to add the word “electronic.” We believe that defining the term “counterfeit electronic part” provides greater clarity, in line with the direction in Section 818(c) to revise the DFARS “to address the detection and avoidance of counterfeit electronic parts,” and in 818(b)(1) “to establish Department-wide definitions of the terms “counterfeit electronic part” and suspect counterfeit electronic part . . . ” (emphasis added). Further, to expand the scope of the rule to include non-electronic products would greatly increase the difficulty and cost of its implementation since test standards and mitigation tools have not yet been developed for non-electronic commodities. This would be particularly burdensome to small businesses that do not have the internal capability or infrastructure to develop counterfeit avoidance standards and test methodologies. At present, data contained in the Government Industry Data Exchange Program does not reflect a severe counterfeiting problem with non-electronic commodities.

Secondly, the definition is missing an intent element. When applied in the context of proposed 231.205-71(b) – (c), the definition effectively creates strict liability for contractors who have provided counterfeit parts, regardless of intent, or care taken to avoid such a result. Even covered contractors who have successfully implemented a government approved counterfeit electronic part avoidance and detection system, but still unknowingly pass such parts to the Government, “are responsible for . . . any rework or corrective action that may be required to remedy the use or inclusion of such parts.” To avoid such harsh consequences, contractors will
likely be forced to take high-cost, time-intensive measures (e.g. redesign or extensive testing), opt for no-bid, or even drop from the government contracting market entirely. This means that if the regulations are finalized as proposed, the government may see fewer competitors, reduced access to technology, more frequent schedule slip, additional redesigns, and cost increases.

By adding an intent element to the definition, however, the strict liability created by the proposed regulations is removed, better positioning contractors to take a balanced, risk-based approach to avoiding and detecting counterfeit electronic parts. This means that a larger number of contractors will be able to stay in the market, compete for greater variety of programs, and keep costs of counterfeit parts prevention commensurate to the risk, all of which contribute to more cost-effective and timely government contract execution. To prevent occurrences of willful blindness or lack of due care in providing electronic parts, we also recommend including in the definition, “reckless” and “negligent” misrepresentation of counterfeit parts, in addition to “knowingly misrepresented”. Our recommended definition reads as follows:

‘Counterfeit Electronic Part means:

(1) an unauthorized a) copy, b) imitation, c) substitute, or d) modified electronic part, which is knowingly, recklessly, or negligently misrepresented as a specified genuine electronic part of an authorized manufacturer; or

(2) a previously used electronic part which has been modified and is knowingly, recklessly, or negligently misrepresented as new without disclosure to the customer that it has been previously used.’

Note – This definition may differ from civil or criminal laws that addresses the acts of counterfeiting or fraud, and is not intended to make a legal determination. Used parts sold as new that have not been modified are not counterfeit according to some civil and criminal statutes. These issues are covered under existing laws covering fraud. For civil matters, this issue would typically be covered under civil fraud and terms and conditions of a purchase order or contract that specifies parts must be new.

At a minimum, we recommend that Subparagraph (3) of the proposed “counterfeit electronic part” definition be stricken, due to several ambiguities that may result in unintended consequences. First, it broadly indicates that a nonconforming item, even one that is wholly unintentional (e.g., a product defect), would be considered counterfeit or suspect counterfeit. Further, out-of-spec escapes that are unintentional and unobserved by the supplier and are represented to the customer “as meeting the performance requirements for the intended use,” would be considered counterfeit or suspect counterfeit. Additionally, while the definition appears to incorporate the expectations of Section 818 to include “previously used parts represented as new,” it also includes “outdated” or “expired” items without offering a definition
for these terms. In many cases, the government needs to buy old, obsolete technology to support weapons systems and the description in the proposed definition may cause confusion and raise unnecessary issues when an obsolete part is offered. For instance, an obsolete but genuine original part carried in distributor inventory and still in use in fielded products could be considered an “outdated” or “expired” item, and thus counterfeit. The terms “intended use” and “end-user” could also introduce problems. It is unclear who determines intended use in the case of an original manufacturer or distributor supplying electronic parts. This term could be plausibly interpreted to mean the supplier, the contractor that has design application knowledge for the electronic part’s “intended use”, or the DoD “end-user”. A component supplier generally does not know what equipment the electronic part will be used in, let alone its “intended use” within that equipment. A component supplier of other than a MIL-Spec item might argue that the item supplied was not intended for use in military equipment at all. The DoD “end-user” would certainly have knowledge for the “intended use” of the equipment containing the electronic part, but would likely not have design application knowledge for the “intended use” for the electronic part within the design of the equipment. These presumably unintended consequences of subparagraph (3) are likely to result in increased costs and schedule impacts for contractors attempting to comply with the rule. Such impacts will likely also be borne by the Government, as contractors are forced to pass them on, or to avoid Government contracting opportunities altogether.

**Suspect Counterfeit Part** –

DFARS Case 2012-D055 Current proposed definition:

*Suspect counterfeit part means a part for which visual inspection, testing, or other information provide reason to believe that a part may be a counterfeit part.*

We believe that the definition of Suspect counterfeit part in proposed 202.101 and 252.246-70XX(a) is overbroad and, when used in the context of 231.205-71(b) – (c), could have significant unintended consequences. As currently proposed, the definition classifies a part as “suspect” if it has any indication, no matter how minute, of being counterfeit. In the context of 231.205-71(b) – (c), a contractor could be forced to expend significant time and costs on reworking or replacing parts that are actually genuine conforming parts, just because there was some minor unsubstantiated suspicion that they were not. These costs and the schedule slip due to required rework could ultimately impact the government, as contractors implement additional actions and infrastructure to mitigate their risk, or drop out of competition for government contracts. In order to avoid such consequences, we suggest using the following definition:

‘Suspect Counterfeit Electronic Part means an electronic part for which there is objective, credible evidence indicating that the part is likely a counterfeit electronic part.’

As clarification, “objective” would be defined as it is commonly understood: information based on facts that can be proved through analysis, measurement, observation, and other such means.
of research and testing or any documented statement of fact, other information, or record, either quantitative or qualitative pertaining to the quality of an item based on observations, measurements, or tests which can be verified.

Even with implementation of a better scoped definition like the one recommended above, we still believe there are implementation issues that need clarification with respect to how the term is applied in the proposed DFARS regulations. While the solutions to these issues are beyond the scope of the DFARS Case 2012-D055 definitions, which this letter mainly addresses, we have some brief recommendations that could be worked into other areas of the proposed DFARS regulations. The DFARS does not address who determines whether a part is suspect, how that determination is made, or what should be done with the part once it is classified as “suspect”. To provide an objective standard for contractors to be judged against, and to avoid the backlog of contractor systems awaiting audit and approval of an acceptable counterfeit part avoidance and detection system, we suggest the rule require contractors to include a self-certification declaration of their compliance with the requirements of the DoD Adopted industry standard AS5553 Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition. Upon this declaration, a contractor would be considered to have an “acceptable system for counterfeit part avoidance and detection”, until determined otherwise. If the contractor has an “acceptable counterfeit electronic part avoidance and detection system”, we suggest it be given the authority to determine if the part is suspect or not. Contractors are more closely connected to their suppliers and the information associated with the parts, and thus best equipped to most cost effectively and efficiently determine the acceptability of parts within their systems. Additionally, covered contractors who have implemented a system to comply with SAE standard AS5553 have inspection and test procedures that allow them to make an accurate determination as to whether the parts are suspect or counterfeit. Further, throughout the industry, most covered contractors are already working to deal with the persistent and evolving threat of counterfeit electronic parts by updating their detection and avoidance systems and preparing for compliance with the impending release of SAE industry standard AS6171 Test Methods Standard; General Requirements, Suspect/Counterfeit Electrical, Electronic, and Electromechanical Parts, which is intended to improve consistency throughout the industry in determining if a part is fit for its use, or classified as “counterfeit” or “used sold as new”. This will likely reduce the Government’s costs required to manage the process, and help avoid time-intensive investigations that would impact schedule.

In addition, to help make the determination of whether a part is “suspect counterfeit”, and to mitigate the risk of inclusion of “counterfeit” or “suspect counterfeit” electronic parts, we recommend that parts acquired from brokers be tested as part of the acceptable counterfeit avoidance and detection system described by proposed 246.870-2, in alignment with the test requirements of the DoD Adopted SAE standard AS6081 Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Independent Distribution, currently invoked by the Defense Logistics Agency’s Qualified Testing Suppliers List (QTSL) Program.
Once an item is designated as “suspect”, we recommend that those parts not be used unless additional testing and investigation can clear the concerns. For parts that are determined to be “counterfeit” or “used sold as new”, we recommend a requirement to quarantine and report through appropriate channels. Moreover, outside of the scope of the DFARS requirements, industry best practices would refer the matter to legal counsel and law enforcement as appropriate and required under law.

Legally Authorized Source –

DFARS Case 2012-D055 Current proposed definition:

Legally authorized source means the current design activity or the original manufacturer or a supplier authorized by the current design activity or the original manufacturer to produce an item.

The definition of Legally Authorized Source in 202.101 and 252.246-70XX(a) is not entirely clear because the word “legally” adds unnecessary complexity. We believe that “legally” is not needed to meet the objectives and intent of the term, and in fact, adds confusion as to how the term should be interpreted. Additionally, we understand the word “design activity” to mean the more common industry term “design authority,” but this is not entirely clear in the definition. To avoid diverting contractors’ efforts to interpreting unnecessary or ambiguous terms, we recommend that the intended meaning be clarified through the following modification:

‘Authorized Manufacturer means the original component manufacturer (OCM) or original equipment manufacturer (OEM), or a source authorized by the OCM/OEM to produce or alter an item.’

Trusted Supplier – Section 818(c)(3) requires that DoD establish a definition for “trusted supplier,” but the proposed rule fails to do so. Creating this definition is critical because thousands of deployed DoD systems require parts for sustainment, but have no original source supply available. This means contractors have to use sources other than original supply to meet contract requirements, but the proposed rule offers neither instruction nor information on how to identify or qualify a “trusted supplier” where no original source is available. Further, there is no instruction on how to determine what additional test or inspection to perform, or what role the Government is to play in source approval. Section 818 recognizes that there are “industry standards” that should guide the qualification of “trusted suppliers” where original sources are not available, yet the proposed rule is completely silent on the subject. In addition, the term “Trusted Supplier” is typically associated with those suppliers approved by Defense MicroElectronics Activity (DMEA) to supply integrated electronics to the U.S. Government for both Trusted and non-sensitive applications. Therefore, we recommend that the term be renamed to “Trustworthy Supplier” to avoid confusion with the “Trusted Suppliers” associated with the DMEA program. We suggest the term be defined in Sections 202.101 and 252.246-70XX(a) as follows:
‘Trustworthy supplier means:

(1) an original manufacturer (Original Component Manufacturer or Original Equipment Manufacturer);

(2) an original manufacturer’s authorized: a) dealer, b) distributor or aftermarket distributor, or c) aftermarket manufacturer who maintains supply chain traceability; or

(3) a supplier under a long-term contract with the contractor who obtains electronic parts exclusively from the sources described in (1) and (2) of this paragraph, and who maintains supply chain traceability.¹

If the term “Trusted supplier” is not changed to “Trustworthy supplier”, we still recommend the same definition be used.

When parts are not available from a “Trustworthy supplier”, we recommend the parts be required to have additional verification and testing, aligned with AS6081 and with what is being developed in the pending G-19A Test Laboratory Standards Development Committee AS6171 standard, as part of an acceptable counterfeit avoidance and detection system under 246.870-2.

We appreciate the opportunity to comment and collaborate with DoD in developing solutions to this very complex issue. Should you have any questions or like to discuss our comments further, please do not hesitate to contact me at (202) 434-8943 or at bmahone@sae.org.

Sincerely,

Bruce L. Mahone
Director, Washington Operations, Aerospace

¹ While supply chain traceability may prove authenticity, it does not prove that the part was properly packaged, stored, or handled in accordance with the OCM’s specification. Although it is out of scope to the DFARS requirements, we recommend that the appropriate Quality Management System be required in accordance with program needs. Covered contractors already have systems in place to manage this concern.