

**COUNCIL OF DEFENSE AND SPACE INDUSTRY ASSOCIATIONS**  
**4401 Wilson Boulevard, Suite 1110**  
**Arlington, Virginia 22203**  
**703-875-8059**

July 15, 2013

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

Re: **DFARS Case 2012-D055**  
CODSIA Case 04-13

Dear Ms. Murphy:

On behalf of the Council of Defense and Space Industry Associations (CODSIA)<sup>1</sup>, we are pleased to submit the following comments on the proposed rule titled "Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055) which was published in the Federal Register on May 16, 2013.

### **Introduction**

CODSIA fully supports the Congressional intent expressed in Section 818 of the FY12 National Defense Authorization Act (NDAA) (Pub. L. 112-81, Dec 31, 2011) to prevent counterfeit electronic parts from entering into products and services sold to the Department of Defense (DoD). Industry has continually focused on improving ways to identify and root out counterfeit parts, regardless of the end user. These efforts have greatly improved the quality and reliability of products and services provided to government customers. The focus of Section 818 on avoiding counterfeit electronic parts already has had a positive overall industry-wide effect, with many companies already having acted to improve their policies and practices.

### **Assumptions**

In developing our comments, CODSIA made certain assumptions, and would ask that you confirm whether you share these same assumptions.

- A strict liability standard of preventing all counterfeit or suspect counterfeit electronic parts from entering the defense supply chain would require covered contractors to greatly enhance supply management oversight given the necessary costs of bearing the

---

<sup>1</sup> CODSIA was formed in 1964 by industry associations with common interests in federal procurement policy issues at the suggestion of the Department of Defense. CODSIA consists of six associations – the Aerospace Industries Association (AIA), the American Council of Engineering Companies (ACEC), the National Defense Industrial Association (NDIA), the Professional Services Council (PSC), The Technology Association of America (TechAmerica), and the U.S. Chamber of Commerce. CODSIA's member associations represent thousands of government contractors nationwide. The Council acts as an institutional focal point for coordination of its members' positions regarding policies, regulations, directives, and procedures that affect them. A decision by any member association to abstain from participation in a particular case is not necessarily an indication of dissent.

risk of remediation should a counterfeit or suspect counterfeit electronic part enter the supply chain.

- There will be continuing demand for electronic parts not available from OEMs or trusted suppliers, leading to higher costs for covered contractors to acquire such parts. Costs of enhanced supply chain assurance, including test and inspection, will increase for covered contractors.
- Additional costs incurred by covered companies to reduce the risk of counterfeit parts, in turn, will be passed on in the form of increased costs to the Government.

### **Government Assessment of Risks in Acquisition Practices**

An essential element that is lacking in this proposal is the recognition that government acquisition practices can be significant contributors to risks and threats in the supply chain and that specific acquisition practices should be diminished or out-right avoided in certain circumstances where the threat of negative mission impact from those risks are heightened. These practices include requirements to drive for lowest price in acquisition and use of lowest-priced, technically acceptable evaluations, to name two. Establishing price as an overriding or predominant factor in acquisitions almost always works against the competitive opportunity of those suppliers that have taken the additional steps necessary to assure their customers of security in their supply chain.

While this particular rule may not serve as the appropriate vehicle to bring about an assessment of those risks and the establishment of guidance to define appropriate use based on the risks identified, CODSIA strongly believes that the overall effort to detect and avoid counterfeit electronic parts will benefit from an assessment of how price-driven acquisition methods discourage investment in supply chain (and cyber) assurance and can cause harm to the industrial base upon which the Department relies.

### **Contradiction to Defense Strategic Guidance**

The Secretary's letter announcing the Defense Strategic Guidance states that the "Joint Force will be prepared to confront and defeat aggression anywhere in the world. It will have the ability to surge and regenerate forces and capabilities, ensuring that we can meet any future threats, by investing in our people and a strong industrial base." The Defense Strategic Guidance further states: "... [I]n adjusting our strategy and attendant force size, the Department will make every effort to maintain an adequate industrial base and our investment in science and technology. . . . To that end, the Department will both encourage a culture of change and be prudent with its "seed corn," balancing reductions necessitated by resource pressures with the imperative to sustain key streams of innovation that may provide major long-term payoffs."

This proposed rule creates barriers to the Department's access to commercial sources and technologies by not exempting commercial items. The proposed rule undermines the vision of the Defense Strategic Guidance by shifting excess and indiscriminate risk and cost to the marketplace, creating barriers to companies that might otherwise seek DoD business. In aggregate, these barriers will force companies to consider carefully whether

they will make or buy solutions, forcing vertical integration to control their supply chain where the risk of external sources is too high or the marketplace is unwilling to provide solutions. Our comments here adhere to the vision of the Defense Strategic Guidance – an industrial base capable of responding to future challenges.

### **Lack of Full Context and Initial Recommendation**

The proposed regulations only implement paragraphs (c) and (f) of Section 818 of the FY 2012 NDAA. Commenting on this rule is rendered more challenging by the fact that at least two other draft rules are in progress that address other elements of the statute, such as improved reporting. This rule is being presented in an uncoordinated, piecemeal fashion, out of context with the full regulatory structure intended to detect and avoid counterfeit parts. CODSIA would recommend that the Department align the release and public comment period of all three rules in order to provide the impacted community and interested public with the opportunity to assess all of the requirements collectively and in context and to better understand how each of these rules will interface with each other. If a coordinated release is not possible, we would request an additional public comment period be afforded after all three rules have been publicly released in order to permit an assessment and response to the entire regulatory schema. If DoD decides to move forward with partial implementation via DFARS Case 2012-D055, we submit for consideration the likely consequences of finalizing the rules as proposed and suggest revisions to mitigate these potential consequences.

### **Lack of Consistency between Regulation and Statute**

Section 231.205-71(c), Contract Cost Principles and Procedures, lists the circumstances under which costs may be allowable for counterfeit electronic parts and the rework or corrective actions associated with their use or inclusion. As currently written, there is a disparity between Part II.B(1) of the supplementary information and Section 231.205-71. As drafted, 231.205-71(c) suggests a narrow exception, where each of three conditions must be satisfied before reimbursement is possible.

While we recognize that it flows from a FY13 legislative change, if adopted as final, Section 231.205-71(c) would conflict with FAR 52.245-1 Government Property, by adding an extra requirement (an operational system to detect and avoid counterfeit parts) that Contractors must meet before they are able to receive equitable adjustment for “Delivery of Government-furnished property in a condition not suitable for its intended use.” This may be viewed as alleviating the Government’s responsibility, as required in the FAR and related case law, to provide conforming material without regard to whether the contractor has an approved operational system to detect and avoid counterfeit parts.

To remedy these inconsistencies and take a more balanced approach for mitigating counterfeit electronic part risks and costs, we suggest a clarification that consistently applies these provisions in any final rule.

### **Risk-Based Approach to Detection and Avoidance**

Section 818 of the FY12 NDAA requires DoD to implement a risk-based approach to minimize the impact of counterfeit electronics, yet the proposed rule does not discuss a risk-based

approach to the detection and avoidance systems industry will be required to implement. Instead, the proposed rule treats all acquisitions of electronic parts equally. Considering the potentially unaffordable costs of “absolute” efforts to detect and avoid counterfeit parts, we believe the rule should encourage industry and government to weigh the odds of occurrence and the potential consequences in responding to potential threats of counterfeit parts.

The consequences of a part being counterfeit can vary dramatically from serious impact on equipment reliability at one end of the spectrum to negligible impact at the opposite extreme. Risk assessments should weigh the consequences of a counterfeit part quality escape and the extent of due diligence applied to prevent an escape. For any part quality escape, the impact on the specific end-use application should be assessed versus the impact – such as cost and schedule delay – of remediation approaches available to address such escape. Some flexibility must be included in the rules and implementation to avoid potentially calamitous results that will occur where the Department demands absolute assurance against counterfeits but the market cannot deliver parts with zero risk.

### **Risk Allocation and Likely Consequences**

Section 818 of the FY12 NDAA includes many requirements both for the DoD and its contractors, because both parties play a role in buying parts for defense systems. Yet the proposed rule allocates nearly all risk and liability for detection and avoidance to prime contractors: “*The intent of section 818 is to hold contractors responsible for detecting and avoiding the use...of counterfeit electronic parts...*” (Emphasis added). Missing is recognition that contractors do not intentionally render parts obsolete and do not decide when to take parts out of production. Nor do contractors determine government decisions on how long to keep aging equipment in inventory. The result is that the Government requires industry to support equipment for which parts are no longer available from original sources or known and trusted suppliers, for example. The Government, in fairness, should share risks with contractors in supplying essential parts that cannot be obtained from original sources or trusted suppliers.

In a review of counterfeit parts reports published through the Government–Industry Data Exchange Program (GIDEP) over the past 11 years, we have found that in every case in which the specific supplier or category of supplier was identified, the part supplier(s) associated with the sale of suspect counterfeit products was an independent distributor or broker. The proposed rule, however, makes higher tier covered contractors legally and financially responsible for acts or omissions of lower-tier suppliers. While Section 818 recognizes that “additional trusted suppliers” must be qualified and used, the proposed rule does not tell industry how it can qualify such suppliers, or what additional tests or inspections to perform if needed parts are otherwise unavailable. Instead, the proposed rule requires prime and upper-tier contractors (often large entities subject to the Cost Accounting Standards) to flowdown responsibility through mandatory contract clauses. Practically, this will prove unworkable because many suppliers, inclusive of commercial manufacturers of devices as well as brokers and distributors, will refuse orders that attempt to flowdown all potential counterfeit liability. Contractors subject to Section 818 do not have the legal authority to mandate that their lower tier vendors accept such flowdown. Requiring the prime contractor to shoulder all risk renders it much more difficult to drive expectations down to where the risk resides. It is not realistic to impose “strict liability” responsibilities on prime and higher tier contractors when they must acquire parts from lower tiers of the supply chain where provenance is less certain and risks can be lowered but not

eliminated. The Government should share in this risk and participate responsibly in source decisions.

Contractors who have acted diligently in attempts to detect and prevent counterfeit parts may still unknowingly pass such parts to the Government. As proposed by this rule, however, these contractors suffer the consequences of a counterfeit escape even where they have taken all responsible acts. This is problematic both because the bad actors that caused the issue are never dealt with and because passing all risk to non-culpable contractors will increase costs and cause schedule impacts for the Government. **Some companies important to the Department, below the level of primes, but in the higher tiers of the supply chain, may choose not to participate in the defense market if they are forced to shoulder excess risk and cost but have no effective means of control over exposure to counterfeit parts.**

The broader impact is that the Government may experience a decline in its ability to complete its missions effectively and affordably. Covered contractors facing a zero-defect rule, which does not take into account the risk of counterfeit parts to the application, will be forced to mitigate the business risk of potentially unlimited exposure to costs of remediation. Their choices include vertical integration, to control sourcing internally, as well as implementation of extensive additional infrastructure and testing. Contractors will propose complete redesign of systems and boards, or insist upon use of contract or re-manufacturing, but the Government may not have the funds to execute these measures. In some cases, especially if the risk of a counterfeit cannot be eliminated, and where the Government absolves itself of any responsibility, covered companies (even at the prime level) will elect to “no-bid.” Moreover, companies lacking the infrastructure to comply with the proposed regulations may be squeezed out of the market entirely and others may decline to assume the costs and risks, resulting in decreased competition and reduced availability of technology for Government contracts.

### **Exercise of Executive Authority**

DoD has acted to create “voluntary disclosures” and agreements that incentivize detection and reporting of issues and mitigate contractor exposure, and the Department of Homeland Security uses the SAFETY Act to limit contractor liability in certain circumstances. Similarly, CODSIA urges DoD to set standards which, when met by industry, will both induce the desired behavior and limit the liability DoD imposes on an otherwise compliant company that inadvertently supplies a counterfeit or suspect counterfeit part, despite due diligence. While the statute makes certain costs unallowable, DoD exercises wide discretion in deciding how broadly to exclude costs. Contractors demonstrating that they have implemented counterfeit prevention policies, and otherwise met Section 818 standards, should be confident that DoD will not impose overly broad cost exclusions.

When the evidence reveals that questioned parts stemmed from an overt criminal enterprise or the work of foreign intelligence attack, the prime contractor’s liability should be limited. Ignoring this marketplace reality of unavoidable overt criminal acts and foreign intelligence attacks inevitably will result in significantly increasing the costs of goods, services and solutions at a time when DoD is focused on affordability.

## **Commercial Item Impact**

The proposed changes do not take into account the handling of commercial items generally and Commercial-Off-the-Shelf (COTS) items specifically. The language of Section 818 is silent about both commercial and COTS items, while report language from the FY13 National Defense Authorization Act specifically requested that the Department address how these categories would be excluded from the requirements of the proposal. It is industry's belief that because there was no reference to these items, in Section 818, it was Congress' intent to exclude commercial and COTS items from the coverage of the statute and any subsequent implementation measures. In line with this, we believe commercial and COTS items purchased directly from OEMs and their authorized distributors should only be held to the requirements of their commercial warranties and any other standard commercial obligations, without the flow-down of the unique requirements in Section 818. The risk of a counterfeit COTS part being counterfeit where purchased from an OEM is comparatively very small.

Most COTS suppliers will provide their standard commercial warranty for the parts they provide; seldom will they provide additional certifications or accept additional liabilities beyond those covered by their commercial warranty (like the strict liability proposed in this rule.) The result of these marketplace realities is that prime or lower-tier contractors that procure COTS items must assume the liability not accepted by the COTS supplier.

## **Definitions**

Generally, the definitions in the proposed rule appear to be consistent with SAE Standard AS5553, "Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition" – in the form as was originally approved by Department in August 2009. Since that time, however, the standard has evolved. Rev. A to AS5553, released in January 2013, takes a different approach to the definition of a "counterfeit" part. Because it is so important that the proposed rule align with industry standards, the Department should consider changes to key definitions.

**Counterfeit Part** – The proposed definition of a "counterfeit" part has three components. The first is that a "counterfeit" part is one that is 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." The definition is critical to the application of proposed 231.205-71(b) – (c), i.e., the portions of the rule that make covered contractors responsible for detecting and avoiding counterfeit parts and for any rework or corrective action, and which make certain costs unallowable.

First, this definition is missing an intent element. In this regard, it differs from the 2013 revision to AS5553 which now defines a "counterfeit" as a "fraudulent" part and "with intent to mislead, deceive or defraud." Because the definition does not require any form of "fault" on the part of the company subject to proposed 231.205-71(b) – (c), its effect is to impose strict liability on such covered contractors – even though they are required to have complaint systems to detect and avoid counterfeit parts by proposed 246.870-1 and by revisions incorporated in purchasing system administration by 252.244-7001. Presumably covered contractors with compliant systems will not intentionally use a counterfeit part, but the present definition makes them responsible for the costs and consequences of other

actors, possibly far downstream in the supply chain, which may have fraudulent intent or acted recklessly.

Under the proposed definition, even covered contractors who have successfully implemented a government approved counterfeit electronic part detection and avoidance 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.” This is fundamentally unfair because no contractor can absolutely eliminate the risk of a counterfeit part any more than the Government can when it purchases for its own account. Moreover, it is the Government that creates the demand for parts that are at the highest risk of being counterfeited and it is the Government that decides whether it will spend the additional money and time required to redesign equipment or otherwise avoid requirements to purchase obsolete or out-of-production parts.

This is why the proposed definition should be revised to incorporate an intent element. If a “counterfeit” part is one that is “fraudulently” created, or “knowingly or recklessly” misrepresented to be genuine, then covered companies who do all that the law requires and have approved, compliant systems will not be punished by unallowable costs of replacement or remediation. They still will be required to have such systems and they still will be responsible for counterfeits that they should have detected or avoided, but they will not be sanctioned or forced to assume potentially unbounded risk for actions outside their control.

Making such a change to the critical definition would mitigate the strict liability otherwise created by the proposed regulations, better positioning contractors to take a balanced, cost-informed, risk-based approach to avoiding and detecting counterfeit electronic parts. This means that more contractors will stay in the market, compete for greater variety of programs, and it will keep costs of counterfeit parts prevention commensurate to the risk, all of which contribute to more cost-effective and timely government contract execution.

We have also identified several ambiguities that may result in unintended consequences. Part (3) of the definition broadly indicates that a nonconforming item, even one that is wholly unintentional (e.g., a product defect), and furnished by its original source, would be considered “counterfeit” or “suspect counterfeit.” This subparagraph does not appear in the corresponding definition within DODI 4140.67 or in the proposed addition to the NASA FAR Supplement.

Out-of-spec escapes could well be unintentional and unobserved by the supplier and the product thus could be represented to the customer “as meeting the performance requirements for the intended use,” which, according to government contract law subject matter experts, could expose the supplier to False Claims Act liability.

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 defining these terms. This implicates a broad variety of circumstances that are presumably not intended to be included in the “counterfeit electronic part” category. For instance, an obsolete but genuine part carried in distributor inventory and still in use in

fielded products could be considered an “outdated” or “expired” item and thus “counterfeit” under this definition.

Use of the terms “intended use” and “end-user” may also introduce confusion. For original manufacturers or distributors supplying electronic parts, who determines “intended use”? Is it the supplier, the contractor that has design application knowledge for the “intended use” for the electronic part; 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 can reasonably contend 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 of the “intended use” for the electronic part within the design of the equipment.

To that end, we recommend the following definition of a counterfeit electronic part:

*An unauthorized copy, imitation, modified or substitute electronic part that has been identified, marked, and/or altered by a source other than the part's legally authorized source and has been fraudulently, knowingly or recklessly misrepresented to be from a legally authorized source, including previously used electronic parts represented as new. Also, an electronic part is an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (Sec. 818(f)(2) of Pub. L. 112-81.)*

Other definitions also need to be modified or clarified.

- **Legally Authorized Source** - This term needs to be clarified. We believe it should specifically include authorized distributors of OEMs. We recommend the following: *the current design activity or the original manufacturer or a supplier authorized by the current design activity or the original manufacturer to produce or distribute 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 clear in the definition either.

- **Suspect Counterfeit Electronic Part:** The definition of “suspect counterfeit part” in proposed 202.101 and 252.246-70XX(a) is unclear and 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 slips 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 Part means an electronic part for which there is objective, credible evidence indicating that the part is likely a counterfeit electronic part.*

Additionally, we suggest that if the Contractor has an “acceptable counterfeit electronic part detection and avoidance system,” it has the authority to determine if the part is suspect or not. Contractors are more closely connected to their suppliers and thus best equipped to effectively determine the acceptability of parts within their systems. The determination of whether a part is “suspect” or “counterfeit,” and the utilization of test measures and methods for this purpose, should be in accordance with current and evolving industry standards. This will likely reduce the Government’s costs required to manage the process, and help avoid time-intensive investigations that would impact schedule.

- **Trusted Supplier** – The proposed rule does not, as Section 818 (c)(3) requires, establish qualification requirements to identify “trusted suppliers” or inform industry how it is to identify and use “additional trusted suppliers” when required parts cannot be obtained from original manufacturers or their authorized distributors (or such “trusted suppliers” who obtain such parts exclusively from them). Literally thousands of deployed DoD systems require parts for sustainment for which *no* supply exists from the original sources. The proposed rule affords zero tolerance for counterfeits even though industry has no choice other than to buy from sources *not* among those the statute identifies as preferred, and the proposed rule offers no guidance as to how to identify or qualify such sources of supply, or what additional test or inspection is required, or what role the customer is to play in source approval. Section 818 refers to “industry standards” that should guide in qualifying “trusted suppliers” if original sources do not exist, yet the proposed rule is silent on this subject. We recommend: “*a supplier that (a) is an original manufacturer, (b) is its authorized distributor, or (c) obtains electronic parts exclusively from the original manufacturer or its authorized distributor*”

We suggest qualifications be established in Sections 202.101 and 252.246-70XX(a) as follows:

‘Trusted supplier means –

- (1) an original manufacturer (Original Component Manufacturer or Original Equipment Manufacturer);
- (2) an original manufacturer’s authorized dealer or distributor who maintains an unbroken chain of custody; 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 an unbroken chain of custody.’

‘Unbroken chain of custody means verifiable evidence of chronological documentation, showing the custody, control, transfer, and traceability of an electronic part to the original manufacturer, and segregation from other sources.’

### **Mandatory Flowdown Clauses for Subcontractors**

The proposed rule should include flowdown clauses and create some standardized terms to better allow prime contractors to equitably distribute responsibility with subcontractors. Restricting all requirements to the prime contractor makes it much more difficult to impose responsibilities down to where the risk can most effectively be mitigated, in the lower tiers of the supply chain. Already, prime and higher-tier contractors are experiencing lower tier suppliers refusal to accept terms and conditions required by Section 818.

Flowdown requirements made explicit should eliminate uncertainty as to responsibility. This can be done by adding a new paragraph to 252.246-70XX, as follows: *“The contractor shall include this clause in all subcontracts or purchase orders at all tiers regardless of value when the subcontract or purchase order contemplates the acquisition of items including electronic parts, except in subcontracts or purchase orders for Commercial Items.”*

Because there will be situations where companies will not be able to secure adherence to the flowdown term from necessary sources in the supply chain, a mechanism must be provided for notification to the Government and relief from the flowdown requirement or other instruction or assumption of responsibility by the Government.

### **Integrating Counterfeit Parts Avoidance into the Purchasing System**

The proposed rule requires that contractors have a Government-approved counterfeit electronic parts detection and avoidance system without establishing criteria for such a system. Lack of criteria renders it difficult for contractors to know how their respective systems will be measured.

Part I in the supplementary information 246.870-1, 246.870-2(b)(9), and 252.246.70XX(b) all mention an “acceptable system for counterfeit part detection and avoidance” or flowdown of such requirement, without pointing to an objective benchmark against which “acceptable” can be evaluated. In the same vein, it is unclear how a contractor is expected to comply with the requirement to develop and implement policies and procedures that “address” each of the areas listed in 246.870-2(b)(1) – (9) and 252.246.70XX(c)(i) – (ix). To provide an objective standard for contractors to be judged against, and to avoid the backlog of Contractor systems awaiting audit and approval, we suggest the rule require contractors to include a self-certification declaration of their compliance with the requirements of industry standard AS5553A. Upon this declaration, a Contractor would be considered to have an “acceptable system for counterfeit part detection and avoidance,” until determined otherwise.

Section 818 requires review and approval of a contractor’s detection and avoidance system with processes “comparable” to those established for contractor business systems. We have major concerns about establishing counterfeit detection and avoidance systems under the actual business systems umbrella. Systems for the detection and avoidance of counterfeits are nascent and we believe it would be inappropriate to treat them in exactly the same way as more well-established systems, such as those for accounting or estimating.

If DoD is determined to include detection and avoidance systems under the business systems rule, however, we are concerned about integrating the counterfeit detection and avoidance system into the already existing purchasing system rather than a standalone, separate system. By making it part of the purchasing system the proposed rule does not take into account the many other relevant functions that are outside of the purchasing function – such as design, engineering, quality assurance, materiel management and accounting, compliance, etc. Making counterfeit avoidance a factor in the adequacy of a purchasing system poses the risk that a counterfeit incident could cause DoD to withdraw purchasing system approval over a matter that is the responsibility of another separate and unrelated technical function. This could literally stop a major contractor in its tracks even if the counterfeit intrusion had nothing to do with purchasing practices and controls.

Section 818(e) requires DoD to implement a program to enhance contractor detection and avoidance of counterfeit electronic parts. At 818(e)(2)(B), such a program is to be accompanied by processes for the review and approval of contractor systems, which processes “shall be comparable to the processes established for contractor business systems”. DoD issued its final Business Systems rule in February 2012. That rule employs a concept of “materiality” as it is intended to address “significant” deficiencies that “materially” affect the ability of DoD to rely on business system information. The remedy of withholding contract payments is imposed where there are “significant deficiencies” and withdrawn when “significant deficiencies” are corrected. The same principle should be applied by DoD in the rules that implement Section 818 and in the oversight mechanism for review and approval of systems to detect and avoid counterfeit electronic parts. DoD does not apply a “zero tolerance” approach to counterfeit elimination in its internal policy, DODI 4140.67 (“DoD Counterfeit Prevention Policy,). Nor does DoD require “perfect” business systems, as evident from the Business Systems rule. Indeed, it would work against DoD’s objectives to apply a “zero tolerance” standard, as concerns counterfeit parts, when the systems to detect and avoid counterfeits are included within several elements of the Quality Assurance and Purchasing business systems, neither of which are subject to such a strict standard.

### **Obsolete and Out-of-Production Parts**

The proposed rule does not yet address (a) known risks and challenges of DoD’s continued use of obsolete and out-of-production parts, (b) the vulnerability created by the continued demand for obsolete and out-of-production parts, (c) the increasing constraints on DoD’s ability to support and fund ways to eliminate continued use of obsolete and out-of-production parts needed to (i) support fielded systems, and (ii) manufacture new orders to aged, legacy designs and specifications. This guidance is needed, as is guidance to industry as to how to handle the demand for obsolete parts and out-of-production parts that cannot be obtained from “trusted suppliers,” and, at the same time, achieve DoD’s goal of avoiding and detecting counterfeit and suspect counterfeit parts.

Some mechanism should also be considered for contractors to assess the bill of materials for products they are supporting to identify when obsolete and out-of-production parts are encountered or anticipated. Contractors also should be encouraged to recommend alternatives to their customer – and should have a right to expect direction from each customer as to how to proceed. DoD also should integrate recognition of its existing “trusted foundry” and “trusted

supplier” programs, giving due consideration for use of these special alternatives if justified and funds are available.

### **Applicability of DFARS Case 2012-D055 and Impact on Small Businesses**

The proposed rule states in the preamble that “There is... the potential for an impact on small entities in the supply chain of a prime contractor with contracts subject to CAS. The impact should be negligible as long as the small entity is not supplying counterfeit electronic parts to the prime contractor.” We do not believe this statement is accurate. This assessment does not consider key impacts on small businesses, such as:

- Significant infrastructure beyond the current industry standard must be put in place (detection, evaluation, reporting) by small businesses to prevent the use/introduction of counterfeit electronic parts, in order to accommodate the statute’s new strict liability standard, as implemented by this rule. Such an expectation poses a significant impact on a small business having to acquire and deploy such additional capabilities. This often will result in small business withdrawal from these business lines.
- Prime contracts will provide increased oversight of small businesses to ensure the requirements of this proposed rule are being met. This will disproportionately affect larger business as contractors cannot assume these small businesses will be able to bear the financial consequences of unintentional introduction of counterfeit parts.

Supplementary Information Part IV also states that “this proposed rule is not expected to have a significant economic impact on a substantial number of small entities . . . because it applies only to contracts that are subject to the Cost Accounting Standards (CAS).” Further, supplementary information Part IV(b) states that “[t]he proposed rule would only apply to prime contractors that must comply with the Cost Accounting Standards . . . .” However, proposed 231.205-71(b) does not make this intent clear. It states that “[c]ontractors that are subject to the Cost Accounting Standards (CAS) . . . and that supply electronic parts or products that include electronic parts under CAS-covered contracts are responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts . . . .” This seems directly at odds with the intention expressed in the supplementary information that proposed rules are meant to apply to CAS-covered prime contracts. By not clearly limiting the application of this proposed regulation specifically to prime contractors, it may be misinterpreted to apply to small businesses and sub-tier contractors without regard to whether they are performing under a CAS-covered contract. Such misinterpretation would be problematic because it is likely to significantly reduce the industrial supply base that is willing and able to create the infrastructure needed to support the requirements in the proposed rule. In turn, reduction in supply base would likely increase costs to the Government and limit the technology available to support its programs. To avoid such a result, we recommend 231.205-71(b) be clarified by adding the word “prime” as follows:

**“Prime** contractors that are subject to the Cost Accounting Standards (CAS) under 41 U.S.C. Chapter 15, as implemented in regulations found at 48 CFR 9903.201-1 (FAR appendix, Cost Accounting Standards)<sup>2</sup> and that supply electronic parts or products that

---

<sup>2</sup> See <http://acquisition.gov/far/97/html/appendix.html>

include electronic parts under **prime** CAS-covered contracts are responsible for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts in such products and for rework or corrective action that may be required to remedy the use or inclusion of such parts.”

Also, we recommend that the requirement for contractors to address the flowdown of “counterfeit detection and avoidance requirements” in proposed 246.870-2(b)(9) and 252.246-70XX(c)(ix) be clarified as follows:

“A contractor’s counterfeit electronic part avoidance and detection system must address, at a minimum, the following areas . . .

The flowdown of counterfeit detection and avoidance requirements to subcontractors **operating under CAS-covered subcontracts.**”

As suggested above, DoD should consider circumstances that may warrant modifying small business participation requirements relating to counterfeit parts avoidance objectives and seek input from higher tier suppliers as to any challenges anticipated in small business participation. Also, flowdown requirements should be subject to relief or modification where it is impossible to fulfill the Government’s requirements because necessary vendors and sources refuse to accept flowdown terms.

### **The Rulemaking Process**

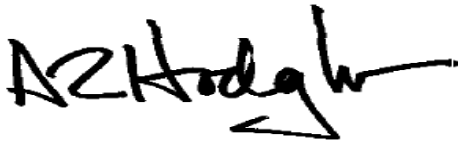
As follow-up to the public meeting held on June 28, 2013, and considering the scope of the rulemaking, CODSIA believes that further effort by both industry and the Department beyond the standard comment collection and analysis process will help achieve the common objective of establishing a manageable and affordable implementation of Section 818 and achievement of its goal of enhanced detection and avoidance of counterfeit electronic parts.

As noted throughout the public meeting, implementing Section 818 is a very complex undertaking which affects many sectors of the defense industry as well as commercial sources that provide necessary technologies. All responsible parties have an interest in protecting against counterfeit parts – but we also share the objective of acting responsibly to minimize costs and avoid adverse impacts to the defense and commercial supply chains. Based on previous experience with other major acquisition rulemakings, CODSIA encourages the DAR Council to host interactive substantive policy meetings between government and industry.

---

We welcome the opportunity to discuss these comments further and to respond to any questions the Council may have. Trey Hodgkins of TechAmerica serves as CODSIA's project lead on this case and he can be reached at 703-284-5310 or at thodgkins@techamerica.org. Bettie McCarthy, CODSIA's administrative officer, serves as an additional point of contact and can be reached at codsia@pscouncil.org or at (703) 875-8059.

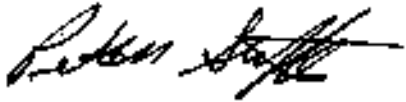
Sincerely,



A.R. "Trey" Hodgkins, III  
Senior Vice President, Global Public Sector  
TechAmerica



Christian Marrone  
Vice President, National Security &  
Acquisition Policy  
Aerospace Industries Association



Peter Steffes  
Vice President, Government Policy  
National Defense Industrial Association



R. Bruce Josten  
Executive Vice President, Government  
Affairs  
U.S. Chamber of Commerce



Richard L. Corrigan  
Policy Committee Representative  
American Council of Engineering Companies



Alan Chvotkin  
Executive Vice President & Counsel  
Professional Services Council