

**DEPARTMENT OF DEFENSE****Defense Acquisition Regulations System****48 CFR Parts 202, 231, 244, 246, and 252**

RIN 0750-AH88

**Defense Federal Acquisition Regulation Supplement: Detection and Avoidance of Counterfeit Electronic Parts (DFARS Case 2012-D055)**

**AGENCY:** Defense Acquisition Regulations System, Department of Defense (DoD).

**ACTION:** Final rule.

**SUMMARY:** DoD is issuing a final rule amending the DFARS in partial implementation of a section of the National Defense Authorization Act for Fiscal Year 2012, and a section of the National Defense Authorization Act for Fiscal Year 2013, relating to the detection and avoidance of counterfeit electronic parts.

**DATES:** Effective May 6, 2014.

**FOR FURTHER INFORMATION CONTACT:** Ms. Amy Williams, telephone 571-372-6106.

**SUPPLEMENTARY INFORMATION:****I. Background**

DoD published a proposed rule in the *Federal Register* at 78 FR 28780 on May 16, 2013, to implement paragraphs (a), (c), and (f) of section 818, entitled “Detection and Avoidance of Counterfeit Electronic Parts,” of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012 (Pub. L. 112-81, enacted December 31, 2011). Paragraph (c) of section 818 requires the issuance of DFARS regulations addressing contractor responsibilities for detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts, the use of trusted suppliers, and requirements for contractors to report counterfeit electronic parts and suspect counterfeit electronic parts. Paragraph (f) of section 818 contains the definitions of “covered contractor” and “electronic part.” Also, paragraph (a) of section 818 requires DoD to provide definitions of “counterfeit electronic part” and “suspect counterfeit electronic part.” Other aspects of section 818 are being implemented separately.

The proposed rule and this final rule also address the amendments to section 818 made by section 833, entitled “Contractor Responsibilities in Regulations Relating to Detection and

Avoidance of Counterfeit Electronic Parts,” of the NDAA for FY 2013 (Pub. L. 112-239, enacted January 2, 2013). Fifty respondents submitted public comments in response to the proposed rule.

After publication of the proposed rule, DoD hosted a public meeting to obtain the views of experts and interested parties in Government and the private sector regarding the electronic parts detection and avoidance coverage proposed for inclusion in the DFARS (see 78 FR 35262, dated June 12, 2013). A dozen representatives of private-sector firms, industry associations, and Government agencies made presentations. Many recommendations were made for improving the definition of counterfeit part, and these were carefully considered in preparing the final rule. Another frequently voiced recommendation was to expand on the nine criteria provided by statute for counterfeit part detection and avoidance systems, a recommendation also acted upon for the final rule. There were many comments made on the applicability of the proposed rule only to Cost Accounting Standards (CAS)-covered contractors and the resultant exemption of small businesses and contracts for the acquisition of commercial items.

**II. Discussion and Analysis**

DoD reviewed the public comments in the development of the final rule. A discussion of the comments and the changes made to the rule as a result of those comments is provided, as follows:

**A. Summary of Significant Changes From Proposed Rule**

- In the definitions at DFARS 202.101 and the clause at DFARS 252.246-7007—
  - The definitions of “counterfeit part” and “suspect counterfeit part” are substantively revised and limited to electronic parts;
  - The definition of “legally authorized source” is deleted; and
  - A new definition of “obsolete part” is added.
- The criteria for a contractor’s counterfeit electronic part detection and avoidance system at DFARS 246.870-2(b) and paragraph (c) of the clause at DFARS 252.246-7007 are expanded and clarified and three new criteria have been added. In addition, the use of a risk-based system by the contractor is clarified.
- Applicability of the counterfeit system criteria only to CAS-covered prime contractors is clarified, as is the required flow down to all subcontractor

tiers providing electronic parts or assemblies containing electronic parts.

**B. Analysis of Public Comments**

## Outline of issues:

1. Comment Period
2. Definitions
  - a. “Counterfeit [Electronic] Part” and “Suspect Counterfeit [Electronic] Part”
  - b. “Trusted Supplier”
  - c. “Legally Authorized Source”
  - d. “Electronic Part”
3. System Criteria
  - a. General
  - b. Training of Personnel
  - c. Inspection and Testing
  - d. Proliferation of Counterfeit Electronic Parts
  - e. Traceability
  - f. Use of Trusted Suppliers
  - g. Reporting and Quarantining
  - h. Suspect Counterfeit Electronic Parts
  - i. Design, Operations, and Maintenance of System
  - j. Flow Down
4. Applicability
  - a. CAS-Covered Contractors
  - b. Commercial Items, Especially COTS Items
  - c. Parts Already on the Shelf
  - d. Other
5. Flowdown Requirements
6. Contractor Purchasing System Review (CPSR)
7. Cost Allowability
8. Industry Standards
9. Testing/Item Unique Identification (IUID) Use
10. Reporting
11. Clauses
12. Obsolete Parts
13. Other Comments

## 1. Comment Period

*Comment:* Five respondents submitted comments on this subject. Three respondents recommended extending the public comment period. One recommended an extension of 12 months, another recommended aligning the comment period for this DFARS rule with that of the two associated FAR proposed rules, and a third respondent recommended delaying this case until formal publication of the report of the Intellectual Property Enforcement Coordinator. Two of these respondents also recommended establishment of a formal Government-industry dialogue to “minimize costs and avoid adverse impacts to . . . supply chains.” A respondent recommended that, given the complexities of this issue, DoD would benefit from issuing a second proposed rule and soliciting additional public comment. However, one respondent argued strongly against any further delay, citing the threats that counterfeit parts pose to warfighters and the country’s economic and physical security.

*Response:* While DoD is aware that many issues associated with

management of the counterfeit parts problem remain to be resolved, DoD cannot afford to wait to take action. Further, the Congress has spoken on counterfeit electronic parts and mandated certain DoD implementation actions in section 818 of the NDAA for FY 2012. All of the possibilities cited by respondents above were considered, and the best course of action was determined to be issuance of this final rule without undue delay. However, a means of accomplishing the suggested Government-industry dialogue is being pursued, and future changes to the DFARS regulations will be considered as they are identified.

## 2. Definitions

### a. “Counterfeit [Electronic] Part” and “Suspect Counterfeit [Electronic] Part”

Twenty three respondents provided comments on the definitions of “counterfeit part” and “suspect counterfeit part.”

#### i. Definition of “Counterfeit Part”

*Comment:* One respondent said that the proposed definition of “counterfeit part” is too broad and allows for undefined and unregulated purchases of electronic parts from sources not authorized by the original manufacturer. Six respondents said that the definition must be limited to electronic parts, i.e., counterfeit electronic parts.” One respondent recommended using the term “item” rather than “part” (see DFARS 202.101 and 252.246–7007).

*Response:* DoD has revised the definition to limit it to electronic parts. The DFARS definition for “electronic part” is the statutory definition included at paragraph (f)(2) of section 818 (see paragraph 2.d. of this section, “Electronic part”). The coverage in this final rule is clearly limited to electronic parts. Therefore, “part” is retained in lieu of “item” in accordance with the language used by the Congress in section 818.

*Comment:* Several respondents cited a preference for the definitions from the SAE AS5553A and (pending) AS6081 standards (“A fraudulent part that has been confirmed to be a copy, imitation, or substitute that has been represented, identified, or marked as genuine, and/or altered by a source without legal right with intent to mislead, deceive, or defraud”). Another respondent suggested that the definition of “counterfeit item” should be the same as that provided in DoDI 4140.67, DoD Counterfeit Prevention Policy.

*Response:* The revised definition takes into account current published agency and industry definitions. Some

changes have been made to bring the DFARS definition in line with the best features of these definitions. However, because of the continually evolving nature of the definitions in industry standards and the inconsistencies among the definitions in the standards, it was not possible to adopt the definitions as included in industry standards. For example, the definition is revised to (1) address the element of intent by adding “misrepresented” and (2) add “unlawful or unauthorized substitution.” Given the wide variety of industry standards and the evolving state of knowledge on the elements needed to be included in a workable definition, it is likely there will continue to be differences between industry standards. Furthermore, using the definition of “counterfeit item” in DoDI 4140.67 verbatim was not feasible because it was developed before the public comment period for this DFARS case and did not benefit from the information provided during the public comment period.

*Comment:* A number of other respondents provided various alternative definitions.

*Response:* DoD carefully reviewed all suggested wording and formulated a comprehensive definition that includes many of the respondents’ recommendations (see response immediately above).

*Comment:* Several respondents commented that the element of “intent” was missing from the definition in the proposed rule, and, as claimed by one of these respondents, the definition therefore is inconsistent with 18 U.S.C. 2320. Another respondent agreed that the definition needs an “intent” element. In the estimation of this respondent, “intent” is especially important because, without it, many more costs become unallowable under the terms of DFARS 231.205–71. Two additional respondents said, by omitting an “intent” element, inadvertent delivery of an incorrect part by a bona fide source could result in liabilities and other obligations that should be limited to situations where there is evidence of intent to mislead or deceive. Another respondent stated that adding an intent element to the definition would mitigate the strict-liability aspect present in the proposed rule. However, the respondent’s proposed definition includes “reckless” and “negligent” “misrepresentation” in addition to “knowingly misrepresented” in order to prevent occurrences of willful blindness or lack of due care. A last element related to “intent” came from a respondent who said that parts that are out of warranty or are genuine but out

of specification or suffer from quality deficiencies should be addressed under the warranty provisions of the contract rather than treated as counterfeit parts.

*Response:* DoD has added an element of intent to the definition of “counterfeit electronic part” by including the term “misrepresented.” Terms indicating supplier failure to exercise appropriate counterfeit detection and avoidance measures, such as “recklessly” and “negligently,” are not included in the definition because they have no bearing on whether the part itself is counterfeit (i.e., supplier negligence cannot change the status of a counterfeit part to a non-counterfeit part).

*Comment:* Many comments addressed one or more of the three parts of the definition in the proposed rule.

Regarding Part 1 of the definition, two respondents noted favorably that it conformed to DoDI 4140.67. Another respondent recommended adding “, reproduction, overrun,” after “copy” and before “or substitute.” A respondent stated that the definition of “legally authorized source” would have to be expanded to include the authorized distributor before the respondent could agree with it.

*Response:* Based on comments received, DoD added to the definition to explain what is meant by “unlawful or unauthorized substitution.” This enabled deletion of the third portion of the “counterfeit” definition in the proposed rule.

*Comment:* With regard to Part 2 of the proposed rule’s definition, a respondent said that it was inconsistent with the intent of the statute and utilized the Lanham Act meanings. Another respondent recommended revising Part 2 to use the term “legally authorizing source” because it would be clearer to apply the term to the source of the item rather than the item itself. A third respondent said that Part 2 constitutes fraud and should be considered in the appropriate areas of law that deal with fraud. Another respondent asked if Part 2 was intended to be different from Part 1. A respondent stated that “intended use” was ambiguous.

Four respondents offered a solution by recommending that Part 2 of the three elements be deleted, given that Part 1, in their estimation, captured the intent of Part 2. A respondent said that an item misrepresented to be an authorized item of the legally authorized source could exclude supply by bona-fide distributors or brokers that acquire excess and out-of-production authentic parts.

*Response:* DoD has revised the definition of “counterfeit electronic part” to list the sources legally

authorized to permit manufacturing or resale of the item (see above responses in this section). In addition, the reference to “intended use” is removed.

*Comment:* Commenting on Part 3 of the definition, one respondent concluded that Part 3 was overbroad because it equated contract-requirements compliance with counterfeiting. This respondent recommended that Part 3 of the definition be struck altogether. A respondent said that it was alright to use “previously used parts represented as new,” but other terms went too far (e.g., new, unused genuine part from the original manufacturer that is discovered to have an unintentional quality issue). Several respondents stated that Part 3 is overly broad because “even newly made parts from original manufacturers that fail acceptance tests would be deemed counterfeits that contractors would be liable for.” One respondent suggested that requiring willful misrepresentation may narrow the scope of the definition appropriately. According to one respondent, basing a counterfeit determination solely on age-related criteria or solely on performance requirements is unnecessary and goes beyond the concerns articulated by Congress. The respondent recommended deleting Part 3 and using a single definition. A respondent proposed to revise Part 3 of the definition to read “(3) A used, outdated, or expired genuine item from any source that is misrepresented to the end user as new or as meeting new part performance requirements” because the revised wording focuses on genuine parts that may not perform as new due to the passage of time or prior misuse. A respondent said that Part 3 of the definition is incorrect because “any source” includes sources that have the right to re-mark, re-label, and reconfigure their device to meet performance specifications. This respondent recommended the following Part 3 language: “A new, used, outdated, or expired item that has been represented, identified, or marked as genuine, and/or altered by a source without legal right as meeting the performance requirements for the intended use.” Another respondent proposed to revise Part 3 into two parts. The respondent, as justification, noted that the AS5553 definition of “counterfeit part” is focused on the misrepresentation of the origin of the part, not its performance with respect to the end user’s requirements, and it is unnecessary to protect the DoD supply chain.

A respondent said that a nonconforming item, even one that is

wholly unintentional and furnished by its original source, would be considered “counterfeit”. Out-of-specification escapes could well be unintentional and unobserved by the supplier and thus represented to the customer “as meeting the performance requirements for the intended use;” this would expose the supplier to False Claims Act liability.

Two respondents were concerned with “misrepresentation” issues. An escape due to a temporary lapse of manufacturing and testing process control could be unintentional and unobserved, these respondents said, and could subject the supplier to False Claims Act liability. Further, “misrepresented” could be misinterpreted manufacturing defects.

Several respondents addressed the use of terms like “new, used, outdated, or expired item.” These respondents said that “outdated” may indicate a date code or lot number that may or may not be equal to either an older or newer date code, and that, left undefined, “expired” could be read to mean packing material such as humidity indicator cards, shelf life that can legitimately be restored in most parts, and other transactions as long as the customer is fully informed and approves. The respondents asked whether an obsolete but original part carried in distributor inventory and still in use in fielded products was considered to be an “outdated” or “expired” item.

Similarly, several respondents raised concerns with regard to “intended use,” asking who determines what the “intended use” is. The respondents said that 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.”

*Response:* DoD addressed concerns about Part 3 of the definition by removing it and including an “intent” element in the revised definition.

*Comment:* A respondent recommended that the definition be revised to delete “from a legally authorized source that is misrepresented by any source to the end user.” Another respondent recommended deleting “from a legally authorized source.” A third respondent said that the definition of “legally authorized source” would have to be revised before the respondent could accept Parts 1 and 2 of the definition. A respondent wondered how a legally authorized source was identified and who gets to decide.

*Response:* DoD is revising the definition of “counterfeit part” to

specify what constitutes the legally authorized source, i.e., the current design activity, the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. The separate definition of that term has been deleted (see also paragraph 2.c. of this section, “Legally authorized source”).

*Comment:* A respondent recommended removing references to substitute equipment because genuine replacement equipment may be “identified (or) marked . . . by a source other than the part’s legally authorized source.” According to the respondent, this could exclude legitimate substitutes for, or alternatives to, original-manufacturer parts due to such circumstances as a legally authorized source no longer producing the equipment. The current definition, the respondent said, could also be interpreted as precluding the use of certain commercially available off-the-shelf (COTS) items.

*Response:* The word “substitute” is replaced with the term “unlawful or unauthorized substitution” in order to distinguish such items from legitimate substitutes.

*Comment:* One respondent suggested replacing “meeting the performance requirements” with “being the current or authorized part.” This respondent also recommended deleting “new” and inserting, between “outdated,” and “or expedited item,” “decommissioned, recalled.”

Two respondents suggested that the final rule provide a definition for “outdated or expired” item. Another respondent recommended defining “authentic part” as “a part manufactured by the original component manufacturer or by a source authorized by the original component manufacturer, including the authorized aftermarket manufacturer.” A respondent asked that the term “source” be revised to “supplier” in two places and “item” to “part” in two places.

*Response:* Part 3 of the proposed definition, which referred to outdated or expired items and items that do not meet performance requirements, is removed. These items, as well as decommissioned and recalled items, fall under the revised definition of counterfeit, which includes “unlawful or unauthorized substitutions.”

ii. Definition of “Suspect Counterfeit [Electronic] Part”

*Comment:* One respondent suggested that DFARS should set forth who has the burden of proof, including

procedures for determination, how it is done, and what should be done with the part once it is classified as “suspect.” This respondent suggested that any part obtained from a non-authorized source be considered a “suspect counterfeit part” if the non-authorized source does not use detection, avoidance, testing, and/or verification processes in accordance with industry standards. One respondent stated its belief that any finding based on testing “can, and should, be supported by ‘visual inspection’ and ‘other information.’”

Several respondents provided alternate definitions. Two respondents declared the definition to be overbroad. Another respondent said that, to be consistent with legal precedents, the definition should be revised as follows: “An electronic part for which there is an indication that it may be Counterfeit based on analysis, testing and/or evidence, although not yet confirmed.” Yet another respondent recommended a revised definition as follows: “An electronic item, or any electronic component thereof, for which visual inspection, testing, or other information provide reason to believe that an electronic part may be a counterfeit item.” A different respondent recommended that the definition should be “one for which there is reasonable cause under the circumstances to believe a part is counterfeit, based on either (1) physical inspection of the part, or (2) credible evidence from other sources.” The respondent considered this to be a better definition because ordinary quality problems could emerge that are treated initially as suspect counterfeit parts but, after investigation, turn out to be otherwise. But, the respondent said, the cost principle at DFARS 231.205–71 would make any costs associated with the item unallowable. Industry should have the authority, according to the respondent, to make a determination whether a part is a “suspect counterfeit” part, and the rule should clarify the processes that should be followed.

*Response:* As with all nonconforming items, the contracting officer is the official responsible for acceptance under the FAR. The definition is revised to include the phrase “credible evidence,” along with examples, to strengthen the fact-based approach. It is not practical or cost effective to test in every case of a suspected counterfeit.

b. “Trusted Supplier”

*Comment:* Nineteen respondents submitted comments requesting a definition for “trusted supplier,” many noting that section 818 relies heavily on the concept of trusted suppliers. Two of

these respondents stated that the law, at section 818(c)(3)(C), requires the regulations to establish qualification requirements pursuant to which DoD may identify trusted suppliers that have appropriate policies and procedures in place to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts. A respondent offered an alternate definition, which was supported by a separate respondent as consistent with SAE industry standards AS5553A and AS6081. A respondent suggested that that term “trustworthy supplier” would be more appropriate and less likely to be confused with other, existing programs. A similar definition was provided by another respondent. Concerns about confusion with other, existing programs were expressed by another respondent, which requested that the DFARS require that companies that are not Defense Microelectronics Activity (DMEA)-accredited trusted suppliers be required to disclose this fact and, further, that the final rule include a statement in the **Federal Register** notice that “clearly underscores that existing requirements to use DMEA-accredited Trusted Suppliers remain in force.”

Other respondents suggested simpler definitions. One respondent recommended that trusted supplier be equated to legally authorized source, as long as these sources were able to document traceability and chain of custody to the original manufacturer.

A respondent recommended that the term “independent suppliers” be used in lieu of “trusted suppliers,” so as not to confuse it with other programs, such as the Trusted Access Program. Another respondent recommended that authorization to purchase electronic parts from trusted suppliers should only be given when it is not possible to purchase the parts from the original manufacturer or sources authorized by the original manufacturer (legally authorized sources).

A respondent pointed out that the DFARS hadn’t defined “supplier” and suggested that the final rule add such a definition. A respondent provided a definition of “authorized distributor.” One respondent stated that it had signed agreements between it and various suppliers that bind the company’s relationship to ensure original manufactured product only is supplied to customers; consideration of these agreements was not included in the proposed rule and, according to the respondent, would unfairly designate authorized distribution as an illegal source. One respondent suggested that use and qualification of trusted

suppliers should be defined by the contractor, not by the Government.

One respondent noted that industry is well aware that it should purchase electronic parts from original manufacturers and their authorized distributors, but this is not always possible because there are thousands of systems in the inventory for which parts remain in demand but are not available from such trusted suppliers.

*Response:* Paragraph (c)(3)(A)(i) of section 818 requires that DoD, and its contractors and subcontractors, whenever possible, obtain electronic parts that are in production or currently available in stock from the original manufacturer, dealers authorized by the original manufacturer, or from trusted suppliers that “obtain such parts exclusively from the original manufacturers of the parts or their authorized dealers.”

Paragraph (c)(3)(A)(ii) of section 818 also permits the acquisition of electronic parts that are not in production or currently available in stock from trusted suppliers. Paragraphs (c)(3)(C) and (c)(3)(D) require DoD and contractors and subcontractors to establish procedures and criteria for the identification of such trusted suppliers. DoD contemplates further implementation with regard to identification of trusted suppliers under DFARS Case 2014–D005.

Paragraph (c)(3)(B) of section 818 requires DoD regulations to establish requirements for notification of DoD and inspection, testing, and authentication of electronic parts that a DoD contractor or subcontractor obtains from any source other than a source identified in paragraph (c)(3)(A).

Therefore, testing or additional inspection is not generally required for electronic parts purchased from the original manufacturer, the design authority, or an original manufacturer-authorized dealer(s). Furthermore, DFARS 252.246–7007(c)(2) specifies that selection of tests and inspection shall be based on minimizing risk to the Government. One of the criteria for determination of risk is the assessed probability of receiving a counterfeit electronic part.

DoD is concerned that defining and using the term “trusted supplier,” or a variation of it, would create confusion due to the use of this term in other, current DoD and industry initiatives. Accordingly, the systems criteria in DFARS are revised to express what is intended by “trusted supplier” without directly using the term, e.g., 252.246–7007(c)(5) uses the phrase “suppliers that meet applicable counterfeit

detection and avoidance system criteria.”

c. “Legally Authorized Source”

*Comment:* Seventeen respondents commented on the definition of “legally authorized source” at DFARS 202.101 in the proposed rule. Many of the comments alleged ambiguity in the definition and expressed concerns about the treatment of millions of parts made by original manufacturers that are in circulation worldwide and are purchased legally by responsible brokers and distributors, parts that are still in demand. Three respondents recommended adding “or distribute” between “produce” and “an item,” in order to capture distributors that have agreements in place with the original manufacturers to distribute items sourced direct from the original manufacturer. Similar changes were recommended by another respondent. Other respondents recommended adding reputable, or authorized, distributors to the definition. Four respondents supported the change with a more strongly worded alternate definition. One of these respondents noted the proposed definition of “legally authorized source” is consistent with the definition of “current design activity” in MIL-STD-130N. A respondent wanted to revise the definition to include licensors of software to clarify that the term applies to both hardware and software.

However, two respondents stated that using the term “legally” added unnecessary complexity to the definition. Another respondent took a different approach, stating that the term “authorized source” needed its own definition. One other respondent was concerned that the current definition could be construed to mean that the actions of an authorized reseller could create a legal liability for the original manufacturer where the reseller integrated third-party components to configure or customize the product at DoD’s direction.

*Response:* DoD has removed the definition of “legally authorized source” and, instead, spelled out at DFARS 246.870–2(b)(5) the entities that are authorized to produce a genuine item, i.e., the original manufacturer, current design activity, or an authorized aftermarket manufacturer.

d. “Electronic Part”

*Comment:* Five respondents provided comments on the definition of electronic part at DFARS 202.101 in the proposed rule. One respondent proposed adding to the end of the definition provided in the statute

(section 818(f)(2)) the phrase “, or materials used to produce assemblies and cables.” Another respondent stated that electronic parts are usually more inclusive than indicated in the proposed rule’s definition. A third respondent recommended that the definition expressly include software, so that there was no opportunity to assume that software was not included. Two other respondents suggested that, for electronic parts where physical marking is not possible and where the risk of counterfeit parts presents a significant mission, security, or safety hazard, DoD should consider requiring “electronic unique identification.”

*Response:* Paragraph (f) of section 818 provided only two definitions, one for “covered contractor” and the other for “electronic part.” The proposed definition directly implements the statutory definition.

However, while retaining the statutory definition, DoD has added to the definition the statement that “The term electronic part includes any embedded software or firmware.”

Requiring electronic unique identification is addressed in paragraph 9.b. of this section, IUID use.

3. System Criteria

a. General

*Comments:* Twenty respondents submitted comments on this subject area. A number of respondents criticized the proposed rule for merely repeating the system criteria from section 818 without elaboration. One respondent said that, while the DFARS requires an operational system, it does not define the approval criteria or specify who will conduct the review or the frequency of reviews. Many of the respondents concluded that the proposed rule did not correctly implement section 818 of the law, specifically the requirement at section 818(b)(2) “to implement a risk-based approach to minimize the impact of counterfeit electronic parts or suspect counterfeit electronic parts on DoD.” In the opinion of some respondents, the proposed rule would impose unreasonable strict liability standards on industry, regardless of significant and good-faith efforts to address the issue. This comment was supported by other respondents that stated, considering the potentially unaffordable costs of treating all acquisitions of electronic parts equally, the final rule should provide for weighing the odds of occurrence and the potential consequences in responding to potential threats of counterfeit parts, which can vary from serious impact to negligible

impact. One of these respondents recommended that DoD enable its largest contractors to take the lead in detection and avoidance of counterfeit electronic parts by allowing those contractors to make risk-based decisions on how best to implement supply chain assurance measures.

A respondent suggested that one way to address the broad-ranging concerns would be to revise DFARS 246.870–2(a) effectively to define a “counterfeit avoidance and detection system” to mean “the contractor’s system for risk analysis based on inspection and testing to mitigate the acquisition and use of counterfeit electronic parts from the supply chain.” The respondent’s use of the term “mitigate” would alleviate the strict liability requirement for 100 percent detection in the proposed rule. A second respondent supported the use of “mitigation” in lieu of a 100 percent avoidance requirement.

*Response:* The final rule adds criteria to the system requirements and expands and clarifies the intent of the criteria in the clause at 252.246–7007. The respondent stating that the DFARS does not define the approval criteria or specify who will conduct the review is referred to FAR subpart 44.3, Contractor Purchasing Systems Reviews, and its supplement, DFARS subpart 244.3. DCMA has developed and published guidance for the conduct of Contractor Purchasing Systems Reviews (CPSRs) that is available on the agency’s Web site. In addition, DCMA is developing a “Counterfeit Detection and Avoidance System Checklist” that will be available when finalized.

The DFARS does take a risk-based approach, as is further clarified in the final rule. DoD has modified DFARS 246.870–2(b) to read, “A counterfeit electronic part detection and avoidance system shall include risk-based policies and procedures that address . . .”. This change conforms the final rule with DoDI 4140.67. The contractor is responsible for establishing a risk-based counterfeit detection and avoidance system with the amount of risk based on the potential for receipt of counterfeit parts from different types of sources. Three additional system criteria are added to the nine criteria set forth in the statute. These criteria are elaborated in the additions to the system criteria that are included in the final rule in the clause at DFARS 252.246–7007.

*Comment:* One respondent made specific suggestions for improving the system criteria at DFARS 246.870–2(b) by requiring the use of “secure mass serialization with alphanumeric tokens for digital authentication” and not

limiting the coverage only to electronic parts.

*Response:* DoD does not endorse specific mechanisms or technology in the rule, but rather focuses on the desired outcome. Furthermore, DoD is restricting initial implementation to electronic parts as specified in section 818, although other items are considered critical and can be subject to counterfeiting.

#### b. Training of Personnel

*Comment:* With regard to DFARS 246.870–2(b)(1) (training of personnel), a respondent noted that the training criteria and the scope of the required training were not identified in the listing of minimum system criteria.

*Response:* DoD agrees with the respondent's statement, but notes that this is an intentional omission. DoD is providing contractors with the flexibility to determine the appropriate type of training required for individual firms, based upon each contractor's assessment of what programs and capabilities are already in place within the firm and the assessment of what more is needed.

#### c. Inspection and Testing

*Comment:* Another respondent, commenting on DFARS 246.870–2(b)(2) (inspection and testing of electronic parts), suggested that DoD provide a listing of minimum inspections and tests.

*Response:* DoD agrees that requiring the contractor to test and inspect all electronic parts would be prohibitive. However, the DFARS does not require all electronic parts to be treated equally. The requirement to test or inspect is dependent on the source of the electronic part. The potential for receipt of counterfeit electronic items is considerably lower when the item is procured from authorized sources and retains traceability. The final rule allows contractors to make risk-based decisions based on supply chain assurance measures.

#### d. Proliferation of Counterfeit Electronic Parts

*Comment:* For DFARS 246.870–2(b)(3) (processes to abolish counterfeit parts proliferation), a respondent commented that DoD should provide minimum requirements for selection of suppliers that include a requirement to purchase products from authorized suppliers whenever possible. Another respondent recommended the addition of the phrase “, such as the quarantine of counterfeit parts.” The respondent stated that this addition would provide a path of legal

justification for quarantining counterfeit parts.

*Response:* DoD has amended DFARS 246.870–2(b)(4) and (b)(6) to address quarantining of counterfeit electronic parts. These criteria are elaborated on in paragraph (c) of the clause at DFARS 252.246–7007.

#### e. Traceability

*Comment:* Multiple respondents commented on the traceability requirements in DFARS 246.870–2(b)(4) (process for maintaining electronic traceability). Two respondents took issue with the perceived significant implementation and compliance problems posed by traceability. One respondent suggested that DoD incorporate a traceability provision that is in accordance with prevailing industry standards to ensure that covered contractors establish and verify the source of electronic parts and the chain of custody. One respondent stated that traceability cannot resolve unreliability concerns and recommended that purchase of electronic parts from an independent supplier should be permitted only after an exhaustive search of all legally authorized sources proved fruitless, and any such purchases must come with required testing. A third respondent stated that the use of the term “mechanisms” required something more than “best practices,” and strongly recommended that DoD establish a technology solution that is proactive and strategic, and one which provides quality, measurable data.

Two other respondents recommended requiring the use of Item Unique Identification (IUID) as a mandatory traceability mechanism.

Another respondent expressed its strong belief that, although the requirement to maintain traceability is taken directly from the statute, it is not realistic to promulgate a zero-tolerance standard. Instead, the respondent recommended that paragraph (b)(4) be revised to make it clear that DoD will be satisfied if a contractor has a system that meets applicable industry standards.

*Response:* DoD intentionally did not mandate specific technology solutions for traceability. The rule provides a contractor flexibility to utilize industry standards and best practices to achieve the required outcome of traceability.

References to IUID marking are added to the final rule as an optional means of maintaining traceability.

With regard to mission-critical electronic parts and electronic parts that could impact human safety, DoD does have a zero-tolerance policy.

#### f. Trusted Suppliers

*Comment:* For DFARS 246.870–2(b)(5) (use and qualification of trusted suppliers), a respondent recommended that it include guidance on what would need to be included in a trusted supplier program. The respondent stated its belief that the Congress intended that a trusted supplier should be one that can demonstrate that it has processes in place to evidence traceability to the original manufacturer or its authorized distributor chain. The respondent stated that, because of the importance of this change to contractors' purchasing systems requirements, any standards imposed by DoD related to trusted suppliers should be subject to notice and comment by industry. A respondent stated that DoD should have a list or checklist of requirements for determining what is a trusted supplier, including auditing processes. Another respondent said that there is a pressing need for industry to receive more guidance about how to handle situations where parts are obsolete or not available from authorized sources or original manufacturers. A third respondent suggested that paragraph (b)(5) would be much improved by adding, at the end, the phrase “as defined by the contractor.”

*Response:* For reasons explained in detail in paragraph 2.b. of this section, “Trusted supplier”, the term “trusted supplier” is not defined in the final rule. However, a categorization of what types of suppliers may be deemed “trusted” and therefore treated differently from other suppliers is included in the system criteria and explained further in paragraph (c) of the clause at DFARS 252.246–7007.

#### g. Reporting and Quarantining

*Comment:* Two respondents commented that DFARS 246.870–2(b)(6) (The reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts) should be revised by adding, at the end, “by use of a global serialized item identifier or IUID per MIL STD 130.” Another respondent referenced section 818(c)(4), (5), and (e)(2)(a)(vi), noting that these provisions directed revision of the DFARS to address reporting requirements, reporting methods, and reporting-related civil liability protections, but paragraph (b)(6) referred only to the requirement to report and did not address the level of reporting detail DoD expects or to whom at DoD or elsewhere the contractor should report. One respondent recommended adding a qualification

that the requirement to report and quarantine didn't come into play until "confirmation of a suspect status by a third-party inspection and, if necessary, testing to the extent of destructive testing of a sample(s)."

*Response:* DoD agrees with respondents who requested additional guidance on reporting and quarantining procedures. The clause at DFARS 252.246-7007 is expanded in the final rule to provide information on where to report, what to report, and the circumstances that require a report. Additionally, the Government plans to address reporting and quarantining requirements more fully in FAR Case 2013-002, Expanded Reporting of Nonconforming Supplies.

#### h. Suspect Counterfeit Electronic Parts

*Comment:* With regard to DFARS 246.870-2(b)(7)(methodologies to identify suspect counterfeit electronic parts and to determine if a suspect counterfeit electronic part is counterfeit), a respondent said that only the original manufacturer, not the prime contractor, can make the determination that a particular part is actually counterfeit, but experience indicates that the original manufacturer will not participate, in most cases, in an investigation. Further, the respondent claimed, it is often more cost effective for both the prime contractor and the Government to declare the parts suspect or scrap and reprocur the parts.

*Response:* DFARS 246.870-2(b)(7) requires the contractor's counterfeit electronic part detection and avoidance system to address methodologies to identify suspect parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit. However, the rule provides the contractor flexibility to employ a risk-based approach to tests and inspections.

#### i. Design, Operations, and Maintenance of System

*Comment:* A respondent commented on DFARS 246.870-2(b)(8) (Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts) and asked whether compliance with industry standards such as AS5553 would fulfill the requirement. Another respondent recommended inserting the phrase "the use and supply of" after "detect and avoid" and before "counterfeit electronic parts."

*Response:* DoD does not specify industry standards in the rule, because industry standards are continually evolving. However, a contractor may elect to use current Government- and

industry-recognized standards to meet this requirement. This clarification has been added to the clause 252.246-7007 in paragraph (c)(8). "Use and supply of" is implied in the current language.

#### j. Flow Down

*Comment:* With regard to DFARS 246.870-2(b)(9) (the flow down of counterfeit detection and avoidance requirements to subcontractors), two respondents recommended the addition, at the end of "including the use of IUID to enable supply chain traceability."

*Response:* Paragraph (b)(9) requires the flow down of all counterfeit detection and avoidance requirements, without the need to specifically identify or list individual requirements. See the response at paragraph 9.b. of this section, IUID use.

#### 4. Applicability

*Comments:* Eighteen respondents submitted comments on applicability.

##### a. CAS-Covered Contractors

*Comments:* Several respondents objected to limiting the applicability of the rule to CAS-covered contractors. Although recognizing that the statute (section 818(f)(1), with reference to section 893(f)(2) of the National Defense Authorization Act for Fiscal Year 2011), defined "covered contractor" to mean a CAS-covered contractor, a respondent expressed concern that limiting applicability to CAS-covered contractors might provide undue risk for the infiltration of counterfeit parts into the DoD supply chain.

Another respondent questioned the exclusion of educational institutions, Federally Funded Research and Development Centers (FFRDCs), and University Associated Research Centers (UARCs) from the new requirements. The respondent stated that the statute does not carve out any of the institutions listed in the proposed rule as exempt from the counterfeit parts strictures. The respondent said that the proposed rule did not sufficiently explain why DoD exempted these institutions and whether they are exempt from the rule even if they are a subcontractor to prime contracts that do include the clause.

Some other respondents, however, interpreted the flowdown requirement not to apply to subcontractors unless the subcontractor also was subject to CAS, leaving, in the opinion of one respondent, a substantial gap in the regulatory coverage.

One of these respondents, for example, stated that "(r)ather than . . . directing counterfeit prevention requirements toward lower-tier

suppliers that tend to be associated with the sale of suspect counterfeit electronic parts, the proposed rule focuses on prime and upper-tier subcontractors (large entities that are subject to CAS) that are not as well positioned to 'eliminate counterfeit electronic parts from the defense supply chain.'" Regardless of this interpretation, these respondents recommended making all subcontractors at all tiers subject to the requirements of the rule.

A respondent noted that the preponderance of sales of counterfeit items is far less than the limits required here and said that it was unclear if subcontracts under the CAS threshold were covered.

One respondent objected that small entities, educational institutions, FFRDCs, and UARCs could be impacted by the rule as subcontractors to CAS-covered prime contractors.

A respondent asked how the regulations would apply to contractors and subcontractors subject to modified-CAS.

*Response:* Section 818 specifically limited to "covered contractors" the applicability of paragraphs—

- (c)(2)(1)(A) (the responsibility for detecting and avoiding the use or inclusion of counterfeit parts or suspect counterfeit electronic parts and for rework or corrective action); and
- (e) (Improvement of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts).

The definition of "covered contractor" at 818(f)(1) referred to the definition at section 893(f)(2) of the National Defense Authorization Act for Fiscal Year 2011, i.e., "the term 'covered contractor' means a contractor that is subject to the cost accounting standards under section 26 of the Office of Federal Procurement Policy Act (41 U.S.C. 422.)" Section 422, in conjunction with the recodification of title 41 of the United States Code, is now sections 1501-1504 of title 41.

As an initial implementation of section 818, this rule has limited application at the prime contract level (including implementation of paragraph (c)(3) of section 818 (Trusted Suppliers)) to CAS-covered contractors.

The final rule does not specifically exempt educational institutions, FFRDCs, and UARCs from application of the rule. Rather, the clause specifies that it does not apply to any contractor that is not CAS-covered pursuant to 41 U.S.C. chapter 15, as implemented in regulations found at 48 CFR 9903.201-1.

The final rule does exclude set-asides for small business from the clause prescriptions for 252.246-7007,

Contractor Counterfeit Electronic Part Detection and Avoidance System (and thus indirectly 252.244–7001, Contractor Purchasing System Administration-Alternative I), because CAS does not apply to contracts with small businesses.

However, all levels of the supply chain have the potential for introducing counterfeit or suspect-counterfeit electronic items into the end items contracted for under a CAS-covered prime contract. The prime contractor cannot bear all responsibility for preventing the introduction of counterfeit parts. By flowing down the prohibitions against counterfeit and suspect counterfeit electronic items and the requirements for systems to detect such parts to all subcontractors that provide electronic parts or assemblies containing electronic parts (without regard to CAS-coverage of the subcontractor), there will be checks instituted at multiple levels within the supply chain, reducing the opportunities for counterfeit parts to slip through into end items. As requested by many respondents, the flowdown requirement is clarified by the addition of a paragraph in the clause at DFARS 252.246–7007 (see also paragraph 5. of this section, Flowdown requirements).

It is correct that small entities, educational institutions, FFRDCs, and UARCS may be impacted by the rule as subcontractors to CAS-covered prime contractors.

With regard to contractors or subcontractors with modified CAS-coverage, the law does not specify a distinction. Therefore any prime contract subject to CAS coverage, whether full or modified, is subject to the final rule.

#### b. Commercial Items, Especially COTS Items

*Comments:* Several respondents questioned making the rule applicable to commercial items in general and commercially available off-the-shelf (COTS) items in particular. One respondent noted that it would not be in DoD's best interest to apply the Government-unique requirements of section 818 to COTS items. Two respondents recommended that, instead, DoD should recognize that commercial and COTS items purchased directly from the original manufacturers and their authorized distributors should be held only to the requirements of the commercial warranties and any other standard commercial obligations. One respondent suggested that, if a COTS item is purchased directly from the original manufacturer, then its

authenticity should not be subject to question. Another respondent stated its belief that the Congress intended to exclude commercial and COTS items from the coverage of the statute.

A respondent concluded that the rule must not be applicable to commercial items because the **Federal Register** notice for the proposed rule did not contain a determination (required by law) that it would not be in the best interest of DoD to exempt commercial items. While agreeing that it was proper to exempt commercial items, the respondent wanted that exemption for commercial items clearly stated in the rule.

*Response:* Section 818 does not specifically address application to contracts or subcontracts for the acquisition of commercial items, either to exempt or to make applicable. However, the provisions of section 818 that require implementation in a contract clause meet the criteria for a covered law subject to 41 U.S.C. 1906 and 1907. That means that DoD shall not apply the clauses to implement section 818 to contracts or subcontracts for the acquisition of commercial items (including COTS items), unless the Director, DPAP, makes a written determination that it would not be in the best interest of the Government to exempt contracts and subcontracts for the acquisition of commercial items (including COTS items) from the applicability of the provisions of section 818.

Therefore, the final rule, like the proposed rule, does not prescribe the clause at 252.246–7007 (and the related clause at 252.244–7001, Alternate I) for use in prime contracts for the acquisition of commercial items (including COTS items). In order to require application to the acquisition of commercial items, it would be necessary to list the clauses at 212.301. However, CAS does not apply to acquisitions of commercial items, and therefore most contractors providing commercial items are not CAS-covered (unless they also provide non-commercial items to the Government under contracts covered by CAS).

The Director, DPAP has determined that the aforementioned clauses in the final rule do apply to subcontracts for the acquisition of commercial items (including COTS items). The proposed rule required at 252.246–7007(c)(9) that the contractor shall flow down counterfeit detection and avoidance requirements to all levels in the supply chain, and did not specify any exceptions. Because this requirement did not specify mandatory flow down of the clause itself, it was not covered by

252.244–7000, which specifies that the contractor is not required to flow down the terms of DFARS clauses in subcontracts for commercial items, unless so specified in the clause. The final rule adds a flowdown paragraph to the clause at 252.246–7007 and makes applicability to subcontracts for commercial items explicit (see paragraph 5. of this section, Flowdown requirement).

Any electronic part procured by a CAS-covered prime contractor is therefore subject to the restrictions concerning counterfeit and suspect counterfeit parts, without regard to whether the purchased part is a commercial or COTS item. Further, studies have shown that a large proportion of proven counterfeit parts were initially purchased as commercial or COTS items.

#### c. 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.

#### d. Other

*Comments:* One respondent objected to limiting applicability to electronic parts and suggested that the rule should apply to all types of DoD purchases. Another respondent wanted to know if the rule was intended to apply only to contractual deliverables or also to "tooling, GSE or other manufacturing aides that are procured with contract funds."

*Response:* DoD is restricting initial implementation to electronic parts as specified in section 818, although other items are considered critical and can be subject to counterfeiting.

*Comments:* One respondent recommended that the final rule apply not only to the acquisition of electronic parts but also to their use, as the latter may well involve software through which malware or exploits are introduced into a company's information technology networks.

*Response:* DoD is not expanding upon the applicability required by the statute, but understands the term "electronic part" to include embedded software. Accordingly, the definition at 202.101 for "electronic part" is revised to add "The term "electronic part" includes any embedded software or firmware."



## 5. Flowdown Requirements

*Comments:* Ten respondents submitted comments on flowdown requirements. Several respondents strongly recommended that the final rule must ensure compliance throughout the supply chain, and the clause must therefore include a mandatory flowdown requirement for use in all subcontracts at every tier. Some of these respondents did note that, even if the requirements were flowed down by prime contractors, there is no way to ensure that a subcontractor would accept the mandatory flowdown. One of these respondents said that “(s)ome 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.” In such cases, the respondent urged that a mechanism be provided for notification to DoD and relief from the flowdown requirement or other instruction or assumption of responsibility by DoD.

Another position was taken by two respondents that recommended that a legally authorized source, including an original manufacturer and distributor that only purchases from an original manufacturer, regardless of what subcontractor tier it might reside at, should not be subjected to the unnecessary costs and man-hours associated with a counterfeit detection and avoidance requirement.

A respondent believed that the flowdown requirement was unnecessary and burdensome and recommended that DoD utilize instead a requirement for compliance with the industry standard AS5553A “that many companies have already implemented.”

*Response:* The final rule flows down the requirements to all subcontractors of prime CAS-covered contractors, at all tiers, without regard to whether the subcontractor itself is subject to CAS or is a commercial item (see also paragraphs 4.a. and 4.b. of this section, CAS-covered contractors and Commercial items (especially CORS items)). DoD has expanded system criterion at (e)(2)(A)(ix) of the statute and clarified the flowdown requirements for the clause at DFARS 252.246–7007 by also adding a flowdown paragraph that applies when the subcontractor is providing electronic parts or assemblies containing electronic parts.

## 6. Contractor Purchasing Systems Review (CPSR)

*Comments:* Fifteen respondents submitted comments on the inclusion of the counterfeit detection and avoidance system as part of the contractor’s purchasing system. Several respondents were dubious that DCMA has the manpower to execute the additional requirements associated with this rule.

*Response:* The DCMA CPSR Group will include a review of the counterfeit electronic parts detection and avoidance system of a contractor when performing a CPSR. The review will include assistance from the local DCMA Quality Assurance Representative. Based on yearly risk assessments and requests from administrative contracting officers (ACOs), the CPSR Group performs as many reviews as possible. A priority determination is considered when preparing the yearly schedule of contractors to be reviewed to mitigate the demand exceeding capabilities.

*Comment:* A respondent noted that section 818 did not specifically require the creation of a new business system or the inclusion of a counterfeit parts detection and avoidance system in an existing business system. This respondent pointed out its interpretation that a contractor’s failure to establish and maintain an acceptable detection and avoidance system could result in disapproval of the contractor’s entire purchasing system and the withholding of payments. Another respondent requested that DoD ensure that a deficiency solely related to the counterfeit part detection and avoidance system would not prevent the overall purchasing system from functioning as if approved. One respondent further requested that the clauses be revised to “make it clear that a ‘significant deficiency’ in a counterfeit system should not result in the imposition of a withhold in addition to any withholds due to such significant deficiency findings in the CPSR system audit.” Several respondents considered that inclusion of the counterfeit parts detection and avoidance system within the purchasing system goes well beyond the intended scope of a contractor’s purchasing system, fails to address the many other contractor systems (e.g., design, engineering, and quality assurance), and fails to acknowledge or incentivize responsible corrective action. If DoD were to proceed as in the proposed rule and retain this as part of the contractor’s purchasing system, then a respondent recommended that any part purchased from a legally authorized source be exempted. Another respondent suggested that contractors be

given wide discretion in their use of industry standards and internal processes to meet goals, particularly with regard to commercial items, and that DoD be given the authority to provide short-term waivers for the introduction of new technology products. Another alternative came from a respondent recommending that the rule include a contractor self-certification declaration of the contractor’s compliance with the AS5553A standard. Two respondents suggested that compliance would be possible if DoD adopted a requirement to capture and authenticate the DoD IUID of each electronic part received from a supplier. (See also section B.9.)

Other respondents stated unequivocally that paragraph (c)(21) of the clause at DFARS 252.244–7001 (the requirement to comply with the counterfeit parts detection and avoidance system (DFARS 246.870–2(b))) could not be met until those requirements are defined with more specificity.

*Response:* If a deficiency is determined by the ACO to be significant in reference to the counterfeit electronic parts detection and avoidance system, the purchasing system may be disapproved, and a withholding of payments can result. There are factors considered by DCMA when making a determination of significance, some of which include public law violations and repeat occurrences.

A CPSR can include the expertise from technical support personnel such as engineering and quality assurance. A contractor’s corrective actions are considered when performing a CPSR, but no incentive program has been developed.

When performing a CPSR, the contractor’s subcontract management policies and procedures are reviewed to ensure they are effective and are being followed. The review will include an examination of the contractor’s policies and procedures related to the detection and avoidance of counterfeit electronic parts.

The definition of legally authorized source is addressed in the definition section of this document. The NDAA for FY 2012 (Pub. L. 112–81) requires that, whenever possible, electronic parts be purchased from original manufacturers, their authorized dealers, or trusted suppliers. DoD reads this requirement as requiring suppliers to have a counterfeit detection and avoidance system that meets the requirements of DFARS 246.870–2(b) and section 818.

The prime contractor is responsible for accepting only non-counterfeit electronic parts from its subcontractors

and suppliers. Requiring electronic unique identification is addressed at section paragraph 9.b. of this section, IUID use.

A CPSR currently ensures compliance with paragraph (c)(21) of DFARS 252.244-7001 by examining the contractor's vendor rating system or equivalent. There is no need for additional definition or clarification.

*Comment:* A respondent recommended that the following sentence be added to paragraph (a) of DFARS 244.303, Extent of review: "Criteria for assessing the adequacy of rationale documenting "commercial item" determinations shall be based on guidance from the DoD Commercial Item Handbook."

*Response:* The respondent's comment is outside the scope of this case.

#### 7. Cost Allowability

*Comments:* Seven respondents submitted comments on the cost allowability section of the proposed rule. The majority of these respondents deemed the cost principle at DFARS 231.205-71 an overreach because it would apply, not just to contractors covered by the Cost Accounting Standards (CAS), but to their suppliers and subcontractors as well. Another respondent read the proposed rule to apply only to a contractor or subcontractor subject to CAS, which argues, at the least, for clarification of the flowdown requirements in the final rule. A respondent stated that the report of the Senate Armed Services Committee assumed "that contractors will recover costs associated with counterfeit part quality escapes from their lower-tier suppliers that provided the counterfeit." This respondent claimed that the Senate Armed Services Committee report and the DFARS proposed rule do not acknowledge realities that a DoD contractor faces.

*Response:* Section 818 paragraph (c)(2)(B) (subsequently modified to provide limited exceptions by section 833 of the NDAA for FY 2013) makes the blanket statement that the regulations shall provide that the cost of counterfeit electronic parts and suspect counterfeit electronic parts and the cost for rework or corrective action that may be required . . . are not allowable costs under Department contracts. This requires treatment in the regulations like any other cost principle. The new cost principle has been located in DFARS subpart 231.2, Contracts with Commercial Organizations. It is therefore applicable to any contract with a commercial organization (i.e., not an educational institution State, local, or federally recognized Indian tribal

government; or a non-profit institution). The cost principles are applied to the pricing of contracts, subcontracts, and modifications to contracts and subcontracts whenever cost analysis is performed, and is used for the determination, negotiation, or allowance of costs when required by a contract clause (see FAR 31.000).

To clarify applicability of the cost principle, the final rule has been modified by removing the statement of contractor responsibility (derived from section 818(c)(2)(A)) that was included in the proposed rule at 231.205-71(b) and could lead to misinterpretation of the applicability of the cost principle.

The prime contractor's responsibility with regard to dealing with unallowable costs incurred by a subcontractor is no different for this cost principle than for any other cost principle.

*Comment:* Two respondents pointed out that the use of "expressly" in the phrase "expressly unallowable" makes the associated costs subject to penalties and, because the statute did not use the term "expressly," suggested that it be removed from the DFARS.

*Response:* DoD has removed the term "expressly" from the final rule. Section 833 does not employ the term "expressly." However, even without the inclusion of the term "expressly" in the regulations, the costs are nevertheless expressly unallowable, because DFARS 231.205-71 explicitly states that the costs are unallowable. Therefore, inclusion of the term is unnecessary.

*Comment:* Some respondents read section 833 to apply only a two-part test, i.e., when (1) the contractor has an approved system or the parts at issue were provided by the Government and (2) timely notice was provided to DoD. However, other respondents read both the statute and DoD as applying a three-part test for allowability. One respondent considered that the use of the conjunctive "and" between the second and third prongs could create ambiguity, given that there is no conjunction between the first and second prongs. Several of these respondents recommended revisions to the cost principle to make it a two-part test rather than a three-part test, as it was expressed in the proposed rule. These respondents also submitted that it would clarify the issue of cost allowability if DoD were to express a preference for purchases from the original manufacturer or a Government procurement center (e.g., the Defense Logistics Agency), thus effectively isolating contractors from any liability associated with such parts.

*Response:* Subsequently, the NDAA for FY 2013 (Pub. L. 112-239) was

enacted on January 2, 2013. It contained section 833, which modified the language of section 818 quoted above, to read as follows:

"(T)he cost of counterfeit electronic parts and suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are not allowable costs under Department contracts, unless—

(i) The covered contractor has an operational system to detect and avoid counterfeit parts and suspect counterfeit electronic parts that has been reviewed and approved by the Department of Defense pursuant to subsection (e)(2)(B);

(ii) the counterfeit electronic parts or suspect counterfeit electronic parts were provided to the contractor as Government property in accordance with part 45 of the Federal Acquisition Regulation; and

(iii) the covered contractor provides timely notice to the Government pursuant to paragraph (4)."

The proposed rule correctly reflects the most recent statutory language, i.e., section 833. Furthermore, review of the legislative history indicated that this structure and resultant meaning was deliberate.

*Comments:* Several respondents proffered other safe-harbor proposals (see also prior comment and response) as follows:

- Change the requirement for notice to the Government from "timely" to "immediate."

- The costs of rework and corrective action should be exempt from the express unallowability of costs if the part was purchased from the original manufacturer or a source authorized by the original manufacturer, or, alternatively, if the contractor "mitigated" (as opposed to "avoided") counterfeit electronic parts.

- When "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."

- A safe harbor should be created for old parts that the original manufacturer no longer manufactures and for which no trusted suppliers have been named.

*Response:* The term "immediate" would institute an unreasonable requirement, and it would not conform to the section 818(c)(4) requirement for the contractor to "report in writing within 60 days to appropriate Government authorities and the Government-Industry Data Exchange Program (or a similar program designated by the Secretary)." Thus, the laws define "timely" as 60 days, not "immediately." Sixty days is also the

time period specified in DoDI 4140.67. DoD agreed that “timely,” as used in DFARS 231.205–71(c)(3), would be clearer if a reference to the 60-day period were added.

The language of section 833 does not allow for the additional exemptions or carve-outs as suggested by respondents.

*Comment:* One respondent noted that, if adopted as final, DFARS 231.205–71(c) would conflict with the clause at FAR 52.245–1, Government Property, by adding an extra requirement (i.e., the requirement at DFARS 231.205–71(c)(1) for the contractor to have an approved, 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. The respondent considered this to have relieved the Government of a responsibility that currently exists within FAR 52.245–1, to provide conforming material without regard to whether the contractor has an approved operational system to detect and avoid counterfeit parts.

*Response:* The requirements of DFARS 231.205–71(c), as written, do not conflict with FAR 52.245–1. First, the clause at FAR 52.245–1 places Government contract property management requirements on the contractor. This clause does not contain terms and conditions related to the allowability of costs (which can found at FAR part 31). Further, the cost principle included at DFARS 231.205–71 is based on the statutory language contained in section 833.

## 8. Industry Standards

*Comments:* Eleven respondents submitted comments on the issue of industry standards. Most of these respondents urged DoD, for its contractors’ use, to adopt industry standards such as SAE AS5553A, entitled “Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition,” which respondents said provided uniform requirements, practices, and methods to mitigate the risk of receiving and installing counterfeit electronic parts, including requirements, practices, and methods related to (i) parts management, (ii) supplier management, (iii) procurement, (iv) inspection, test, and evaluation, and (v) response strategies when suspect counterfeit electronic parts are discovered. One respondent stated that DoD and NASA already have adopted the AS5553A standard for their own use. Another respondent recommended that AS5553A be used to delineate detection and avoidance system criteria

by express reference to industry standards. A respondent noted that the use of a standard-based approach would be technology neutral and afford industry with a variety of choices that enable flexibility in implementation rather than imposing rigid and potentially harmful Government regulations. Using the available industry standards, according to another respondent, would consider source, traceability, part application, risk assessment, and testing requirements. Some of these respondents noted that current industry standards, e.g., AS5553A, require processes to prevent the reintroduction of counterfeit and suspect counterfeit parts back into the supply chain. If AS5553A were adopted, a respondent said, then contractors should be allowed to self-certify their compliance with the standard; upon such self-certification, a contractor should be considered to have an acceptable system for counterfeit part detection and avoidance, until determined otherwise.

Other respondents focused on the “secondary market,” i.e., distributors and brokers, stating that these types of sources are necessary. These respondents recommended that covered contractors should be encouraged, if not required, to impose known industry standards, such as AS5553A, AS6081, or AS6171 on their secondary market sources and small business suppliers.

A cautionary note was struck, however, by one respondent, which stated that industry standards on counterfeit parts currently vary and continue to evolve in response to industry advances, requirements, and applicable regulations, which might lead to the risk of procurements involving the same part specifying different standards. Another respondent recommended the use of industry standards, including IDEA–STD–1010 as well as AS5553A and AS6081, but cautioned that there are still many artifacts and characteristics found under inspection that remain controversial. The respondent provided examples, such as “striations on the body of an electronic part due to normal shuffling within the product’s protective carrier during transportation (or) authorized remarking of a part by the/an authorizing entity.”

*Response:* DoD concurs that industry consensus standards could be used for the development and implementation of internal counterfeit parts detection and avoidance systems. It is Government policy to participate on industry standard writing bodies (see OMB Circular A–119) and Government/industry conformity assessment

initiatives (see 15 CFR Part 287, Guidance on Federal Conformity Assessment Activities) and to adopt industry standards wherever practical. DoD will continue to be an active participant on industry counterfeit avoidance standard-writing bodies. An additional system criterion is added to DFARS 246.870–2(b) to require contractors to have a process for keeping continually informed of current counterfeiting information and trends. However, DoD agrees with the respondent noting that industry standards on counterfeit parts currently vary and continue to evolve. For this reason, DoD has not mandated the use of specific industry standards but left their use to the contractor, and DoD has not adopted the still-changing definitions in industry standards.

## 9. Testing/IUID Use

In this category, eight respondents submitted comments.

### a. Testing

*Comments:* 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, one respondent recommended that “parts acquired from brokers be tested as part of the acceptable counterfeit avoidance and detection system described by proposed DFARS 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.” Another respondent recommended testing of all items, parts, and components when they are received by the procuring entity.

*Response:* DoD agrees with the respondent’s recommendation to specify testing requirements when parts are procured from sources that present elevated risk. Appropriate text is added in the system criteria at DFARS 246.870–2(b) and the clause at DFARS 252.246–7007.

### b. IUID Use

*Comments:* Many respondents stated their belief that the detection and avoidance of counterfeit electronic parts is predicated on the successful implementation of Item Unique Identification (IUID) for each electronic part. Several of the respondents noted that considerable policy already exists in DoD that could be leveraged to assist with the identification of counterfeit

electronic parts. The respondents cited the required use of automatic identification technology (AIT) or automatic identification and data capture (AIDC) technologies, and some cited, in support, GAO report GAO-10-389, entitled "DoD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts." Two of these respondents referred to section 807, Sense of Congress on the Continuing Progress of the Department of Defense in Implementing its Item Unique Identification Initiative, of the NDAA for FY 2013. The Congress found that IUID "has the potential for realizing significant cost savings and improving the management of defense equipment and supplier throughout their life cycle" (section 807(a)(2)), as well as being able to "help the Department combat the growing problem of counterfeit parts in the military supply chain" (section 807(a)(3)). These respondents stated that requiring suppliers to assign IUIDs to electronic parts and register those parts in the DoD IUID Registry would better enable contractors to verify their sources as part of a contractor purchasing system review. The respondents noted that DoD has a policy that supports serialized item management for material maintenance (DoDI 4151.19), and another policy, at DoDI 8320.04, that requires any DoD serially managed items to be marked with an IUID-compliant mark. Further, one of the respondents stated that DoD's IUID policy requires the use of the IUID Registry, which includes, along with the Unique Item Identifier, pedigree data. A major component of the pedigree data, according to the respondent, is the Enterprise Identifier (EID), which mostly corresponds to the original item manufacturer. For electronic parts where physical marking is not possible, two respondents said that technology exists and standards are evolving for electronic unique identification.

*Response:* DoD concurs with the benefits of item unique identification (IUID) described by the respondents. DoDI 4140.67 requires DoD component heads to "(a)pply item unique identification (IUID) using unique item identifier (UII) for critical materiel identified as susceptible to counterfeiting to enable authoritative life-cycle traceability and authentication." For purposes of this final rule, DoD focused on the desired outcome of traceability without mandating the means to achieve the outcome.

Currently, the clause at DFARS 252.211-7003, Item Identification and Valuation, requires an IUID for items

with an acquisition cost of \$5,000 or more. In an individual contract, the DoD may request assignment of an IUID for items with a lower acquisition cost, when identified by the requiring activity as critical materiel identified as susceptible to counterfeiting, serially managed, mission essential, or controlled inventory, or the requiring activity determines that permanent identification is required. IUID marking and registry is already required by the DFARS for electronic items that meet those criteria (see DFARS 211.274).

A complete discussion of DoD's IUID system is found at [http://www.acq.osd.mil/dpap/pdi/uid/data\\_submission.information.html](http://www.acq.osd.mil/dpap/pdi/uid/data_submission.information.html). The registry, located on the Internet at <https://www.bpn.gov/iuid>, is an acquisition gateway to identify (a) what the item is; (b) how and when it was acquired; (c) the initial value of the item; (d) current custody (Government or contractor); and (e) how it is marked.

#### 10. Reporting

*Comment:* A respondent recommended revisions to DFARS 246.870-2(b)(6) and the clause at 252.246-7007(c)(iv) to include specific reporting requirements consistent with the current reporting of possible violations of a contractor's code of business ethics and conduct (DFARS 203.1003(b)). The respondent's recommended change would revise the text as follows:

"The reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts, in writing, to the contracting officer and the Department of Defense Inspector General, in accordance with DFARS 203.1003(b), within 60 days of identifying the counterfeit or suspect counterfeit electronic parts."

*Response:* Not all counterfeit or suspect counterfeit parts are due to fraud, and, in any case, reporting of fraudulent activity to the DoD IG is already required by various DoD and Governmentwide clauses and provisions. FAR Case 2013-002, Enhanced Reporting of Nonconforming Parts, has been opened to further address reporting requirements. In that case, the requirements to report to the contracting officer and to the Government-Industry Data Exchange Program (GIDEP) will be clear, as is the existing requirement (at other parts of the FAR and DFARS) to report fraud to the IG. 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."

*Comment:* A respondent recommended adding, at DFARS 246.870-2(b)(6), to whom the occurrence (of a counterfeit or suspect counterfeit electronic part) must be reported and within what period of time it must be reported. The respondent wanted to know whether it would be acceptable to report to industry associations, law enforcement, or other organizations in other countries if the counterfeit was discovered outside the U.S.

*Response:* In accordance with section 818, the reporting is intended to be made to GIDEP within 60 days, but these requirements are being addressed in a FAR case (2013-002, Expanded Reporting of Nonconforming Items) that had not been released for public comment at the time the public comment closed for this DFARS case. The FAR signatories intend for all such reports to be made to GIDEP, regardless of where the counterfeit was identified.

*Comment:* A respondent noted that Congress was insistent on improved reporting by DoD and industry and said that it is through reporting that industry and Government inform each other of known risks and identified threats. The respondent acknowledged that a draft FAR case (2013-002) will address reporting, but the DFARS rule essentially ignored reporting. The respondent expressed concern about anecdotal evidence of lower reporting to the GIDEP since enactment of section 818 and urged DoD to conduct a review of reporting frequency to GIDEP subsequent to December 13, 2011.

*Response:* The frequency of reports made to GIDEP is outside the scope of this case.

#### 11. Clauses

*Comment:* A respondent recommended reversing the order of the words "detection" and "avoidance" in the clause title of 252.246-7007 and in lines 3 and 5 of paragraph (b), so as to reflect the actual process, i.e., one cannot avoid what one has not detected.

*Response:* DoD has made appropriate revisions to DFARS 246.870-2 and -3 and the clauses at 252.244-7001, its Alternate I, and 252.244-7007.

*Comment:* One respondent recommended revising the prescription for the clause at FAR 52.246-7007 to add statutory references and references to the Code of Federal Regulations.

*Response:* The clause prescription is revised to ensure the clarity of its applicability, but statutory references and references to the CFR generally are not included in clause prescriptions.

## 12. Obsolete Parts

*Comment:* One respondent stated that the issue of obsolete parts must be addressed, possibly through a definition for “obsolete part.” Noting that electronic parts have life cycles far shorter than the defense and aerospace products utilizing them, the respondent said that it is incumbent on DoD to provide clear guidance so that contractors can develop supply chain processes to mitigate risks inherent with obsolete parts requisitioning.

*Response:* The following definition of “obsolete electronic part” is added in the final rule: “An electronic part that is no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the design activity or original manufacturer.” Obsolescence control is a fundamental aspect of counterfeit prevention and should be addressed by the contractor in its counterfeit detection and avoidance system (see DFARS 246.870–2(b)(12) and paragraph (c)(12) of the clause at DFARS 252.246–7007).

*Comments:* Several respondents expressed concerns about obsolete parts. One respondent stated that the rule should 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 respondent recommended some mechanism for contractors to assess the bill of materials for products being supported, recommend alternatives, and expect direction from each DoD customer as to how to proceed.

A respondent recommended that contractors be instructed to purchase directly from legally authorized sources. The respondent recognized, however, that there may be circumstances where a part is unavailable from any legally authorized source, including authorized aftermarket sources, and recommended that, after a contractor in good faith determines this to be the case, it should be permitted to purchase a part from a “trusted supplier.” Another respondent stated that DoD had not recognized the role parts brokers play in supplying obsolete parts for long life-cycle DoD systems when the original manufacturer

has discontinued manufacturing a part long before a system is retired.

*Response:* Parts obsolescence is a matter of concern because it can create vulnerabilities in the supply chain. DoD is adding a definition of “obsolete electronic part” in the final rule, and the system criteria at DFARS 246.870–2(b) and 252.246–7007(c)(12) are modified to address obsolete parts. Detailed guidance and mechanisms concerning supply chain processes to mitigate risks inherent with obsolete parts are outside the scope of this case. Guidance and mechanisms concerning obsolete parts mitigation are discussed collaboratively via the Government’s Diminishing Manufacturing and Material Shortages (DMSMS) Program and its Knowledge Sharing Portal. See <https://acc.dau.mil/dmsms>.

## 13. Other Comments

*Comment:* Recognizing that DoD was constrained by the terms of the legislation in drafting this rule, a respondent recommended that DoD push in the future for a legislative change that the respondent considered would give DoD and its contractors an opportunity to establish plans for addressing part obsolescence and balance the cost of design modifications to eliminate obsolete parts against the risk of purchasing obsolete parts from riskier sources of supply.

*Response:* Legislative proposals are outside the scope of this case.

*Comment:* A respondent noted that a large challenge will be to ensure adequate workforce training across the Federal Government.

*Response:* The determination and provision of appropriate training for the DoD workforce is outside the scope of this rule and is being assessed by the Defense Acquisition University.

*Comments:* Three respondents provided information about their products that they assert are proven and acceptable methods for detecting counterfeit parts and rapidly determining if a suspect part is, in fact, counterfeit.

*Response:* DoD does not advocate for individual products.

*Comment:* A respondent noted that a major rule is defined as one that is likely to result in (a) an annual effect on the economy of \$100 million or more, (b) a major increase in cost or prices for consumers, individual industries, Federal, State, or local government agencies, or geographic regions, or (c) significant adverse effects on competition, employment, investment, productivity, innovation, or on the ability of the U.S.-based firms to compete with foreign-based firms in

domestic and export markets. Given the definition, the respondent suggested that DoD should reexamine whether this rule should be re-classified as a major rule because of the potential for understatement as a result of the flowdown requirement to all subtiers.

*Response:* DoD has reassessed the cost impact of this rule and does not consider that it meets the criteria for classification as a major rule. The Office of Information and Regulatory Affairs also did not find this rule to be a major rule.

## C. Other Changes

The proposed rule contained a definition of “counterfeit electronic part avoidance and detection system” in the clause at DFARS 252.246–7007. Because the revisions and extensive additions made in the final rule to the system criteria at DFARS 246.870–2(b) and the clause at DFARS 252.246–7007 effectively define this system more thoroughly than did the definition in the proposed rule, the definition has been removed from the clause in the final rule.

## III. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. This is a significant regulatory action and, therefore, was subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993. This rule is not a major rule under 5 U.S.C. 804.

## IV. Regulatory Flexibility Act

A final regulatory flexibility analysis has been prepared consistent with the Regulatory Flexibility Act, 5 U.S.C. 601, *et seq.*, and is summarized as follows:

This final rule partially implements section 818 of the National Defense Authorization Act for Fiscal Year 2012 and implements section 833 of the National Defense Authorization Act for Fiscal Year 2013 in DoD-wide regulations on contractors’ requirements to identify, avoid, and report counterfeit and suspect counterfeit parts.

No significant issues were raised by the public with regard to the initial regulatory flexibility analysis. However,

several respondents commented in favor of, or against, flowing down the counterfeit parts detection and avoidance system required of prime CAS-covered contractors to small business suppliers. Small business subcontractors that supply electronic parts or assemblies containing electronic parts to CAS-covered prime contractors will incur some costs for complying with prime contractors' requirements.

No comments were received from the Chief Counsel for Advocacy of the Small Business Administration.

The rule does not apply to small entities as prime contractors. The requirements apply only to 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. Prime contracts with small entities are exempt from CAS requirements.

There is, however, the potential for an impact on small entities in the supply chain of a CAS-covered prime contractor, but only when the prime contractor is supplying electronic parts or assemblies containing electronic parts and the subcontractor is also supplying electronic parts or assemblies containing electronic parts. In that case, the prohibitions against counterfeit and suspect counterfeit electronic items and the requirements for systems to detect such parts flow down to all levels of the supply chain. There will, therefore, be some impact on small entities that supply electronic parts to DoD CAS-covered prime contractors but no impact on small entities when they supply electronic parts directly to DoD.

The rule uses the existing requirements for contractors' purchasing systems as the basis for the anti-counterfeiting compliance (see the clause at DFARS 252.244–7001, Contractor Purchasing System Administration, and its Alternate I).

Suppliers, including small entities, will need to be able to trace the source of the electronic parts they are supplying to the original source if they are not the original manufacturer or current design activity, including an authorized aftermarket manufacturer.

The economic impact on small entities has been minimized by—

(a) Using the existing requirements (and contract clause) for contractors' purchasing systems, rather than creating separate, new systems; and

(b) Restraining applicability only to small businesses that are subcontractors supplying electronic parts or assemblies containing electronic parts to CAS-covered prime contractors.

Seven comments were received on the Regulatory Flexibility Act section during the public comment period:

*Comments:* Several respondents concluded that, because small business suppliers are part of every CAS-covered contractor's supply chain, small businesses will be impacted by this rule, even though they would otherwise be exempted as prime contractors (not subject to CAS). Despite the different impact on small businesses as subcontractors/suppliers versus small businesses as prime contractors, one of these respondents stated that it was important to make the clause at DFARS 252.246–7007 a mandatory flowdown requirement for use in all subcontracts at every tier. However, a different respondent strongly recommended that the impact on small businesses should be minimized by clarifying the applicability of the cost allowability limitations to prime CAS-covered contractors and limiting the flowdown of counterfeit detection and avoidance requirements to subcontractors operating under CAS-covered subcontracts. A third respondent approached this subject by noting that, “(a)nalytically, DoD should be just as concerned about the impact of a counterfeit from a small business as from a large contractor . . . (b)ut important socio-economic policies are served by small business participation requirements.” This respondent favored flowdown to all subcontractors/suppliers but suggested that DoD fashion some sort of safety valve to address situations where the only sources of required parts refuse to accept flowdown and won't agree to conform to risk-mitigation requirements.

Other respondents stated that the impact on small business subcontractors/suppliers would not be negligible because the flowdown of counterfeit detection and avoidance requirements will always have costs. The proposed rule would require all affected subcontractors, including small businesses, to incur substantial overhead costs to establish the necessary compliance systems, according to one respondent. Two other respondents stated that the impact on small entities would likely be significant, either due to the associated costs of detection and avoidance or the inability to compete without such capabilities.

*Response:* DoD agrees with those respondents that deemed small businesses will be impacted as subcontractors. The requirement for flowdown is addressed in a previous section of this rule. However, affected subcontractors, including small

businesses, will not necessarily incur substantial new overhead costs to establish necessary compliance systems, as suggested by some respondents. Most firms that produce or distribute electronic parts or assemblies containing electronic parts are well aware of their obligation not to furnish counterfeit electronic parts and have programs in place to protect themselves and their customers from the consequences of counterfeit parts. DoD's analysis of the impact of this rule on small businesses reflects this circumstance.

## V. Paperwork Reduction Act

This rule affects the information collection requirements in the provisions at DFARS subpart 244.3 and the clause at DFARS 252.244–7001, currently approved under OMB Control Number 0704–0253, entitled Purchasing Systems, in accordance with the Paperwork Reduction Act (44 U.S.C. chapter 35). The current information collection estimates that 90 respondents will submit one response annually, with 16 hours per response. We estimate that the additional information collection burden associated with the clause at 52.244–7001—Alternate, will be as much as five percent more than the existing burden. Therefore, the change to the current annual reporting burden for OMB Control Number 0704–0253 is estimated as follows:

*Respondents:* 5.

*Responses per respondent:* 1.

*Total annual responses:* 5.

*Preparation hours per response:* 16.

*Total hours:* 80.

One comment was received on the Paperwork Reduction Act section of the proposed rule:

*Comment:* A respondent noted that the numbers submitted in the proposed rule estimated that DCMA would conduct 90 CPSRs annually and that, if these numbers were accurate, then DCMA would be unable to complete audits of all 1,200 CAS- and partial-CAS-covered contractors for a first-time audit of their counterfeit parts enhancements for over a decade. In addition, the respondent said, the DoD estimate did not factor in the cost and paperwork associated with the enhanced CPSRs for the other potentially impacted subcontractors, which it claimed could number in the tens of thousands.

*Response:* A complete CPSR is not always necessary for all contractors. Further, DCMA continually assesses its oversight obligations and modifies its priorities and assignments as required.

## List of Subjects in 48 CFR Parts 202, 231, 244, 246, and 252

Government procurement.

### Manuel Quinones,

Editor, Defense Acquisition Regulations System.

Therefore, 48 CFR parts 202, 231, 244, 246, and 252 are amended as follows:

■ 1. The authority citation for 48 CFR parts 202, 231, 244, 246, and 252 continues to read as follows:

**Authority:** 41 U.S.C. 1303 and 48 CFR chapter 1.

### PART 202—DEFINITIONS OF WORDS AND TERMS

■ 2. In section 202.101 add, in alphabetical order, the definitions “counterfeit electronic part,” “electronic part,” “obsolete electronic part,” and “suspect counterfeit electronic part” to read as follows:

#### 202.101 Definitions.

\* \* \* \* \*

*Counterfeit electronic part* means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

\* \* \* \* \*

*Electronic part* means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (section 818(f)(2) of Pub. L. 112–81). The term “electronic part” includes any embedded software or firmware.

\* \* \* \* \*

*Obsolete electronic part* means an electronic part that is no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the current design activity or original manufacturer.

\* \* \* \* \*

*Suspect counterfeit electronic part* means an electronic part for which credible evidence (including, but not limited to, visual inspection or testing)

provides reasonable doubt that the electronic part is authentic.

\* \* \* \* \*

### PART 231—CONTRACT COST PRINCIPLES AND PROCEDURES

■ 3. Add section 231.205–71 to read as follows:

231.205–71 Cost of remedy for use or inclusion of counterfeit electronic parts and suspect counterfeit electronic parts.

(a) *Scope.* This subsection implements the requirements of section 818(c)(2), National Defense Authorization Act for Fiscal Year 2012 (Pub. L. 112–81) and section 833, National Defense Authorization Act for Fiscal Year 2013 (Pub. L. 112–239).

(b) The costs of counterfeit electronic parts or suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are unallowable, unless—

(1) The contractor has an operational system to detect and avoid counterfeit parts and suspect counterfeit electronic parts that has been reviewed and approved by DoD pursuant to 244.303;

(2) The counterfeit electronic parts or suspect counterfeit electronic parts are Government-furnished property as defined in FAR 45.101; and

(3) The contractor provides timely (i.e., within 60 days after the contractor becomes aware) notice to the Government.

### PART 244—SUBCONTRACTING POLICIES AND PROCEDURES

■ 4. In section 244.303, designate the text as paragraph (a) and add a new paragraph (b) to read as follows:

#### 244.303 Extent of review.

\* \* \* \* \*

(b) Also review the adequacy of the contractor’s counterfeit electronic part detection and avoidance system under clause 252.246–7007, Contractor Counterfeit Electronic Part Detection and Avoidance System.

■ 5. Revise section 244.305–71 to read as follows:

#### 244.305–71 Contract clause.

Use the Contractor Purchasing System Administration basic clause or its alternate as follows:

(a) Use the clause at 252.244–7001, Contractor Purchasing System Administration—Basic, in solicitations and contracts containing the clause at FAR 52.244–2, Subcontracts.

(b) Use the clause at 252.244–7001, Contractor Purchasing System Administration—Alternate I, in

solicitations and contracts that contain the clause at 252.246–7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, but do not contain FAR 52.244–2, Subcontracts.

### PART 246—QUALITY ASSURANCE

■ 6. Add subpart 246.8 to read as follows:

#### Subpart 246.8—Contractor Liability for Loss of or Damage to Property of the Government

Sec.

246.870 Contractors’ counterfeit electronic part detection and avoidance systems.

246.870–1 Scope.

246.870–2 Policy.

246.870–3 Contract clause.

#### Subpart 246.8—Contractor Liability for Loss of or Damage to Property of the Government

##### 246.870 Contractors’ counterfeit electronic part detection and avoidance systems.

##### 246.870–1 Scope.

This section—

(a) Implements section 818(c) of the National Defense Authorization Act for Fiscal Year 2012 (Pub. L. 112–81); and

(b) Prescribes policy and procedures for preventing counterfeit electronic parts and suspect counterfeit electronic parts from entering the supply chain when procuring electronic parts or end items, components, parts, or assemblies that contain electronic parts.

##### 246.870–2 Policy.

(a) *General.* Contractors that are subject to the Cost Accounting Standards (CAS) and that supply electronic parts or products that include electronic parts and their subcontractors that supply electronic parts or products that include electronic parts, are required to establish and maintain an acceptable counterfeit electronic part detection and avoidance system. Failure to do so may result in disapproval of the purchasing system by the contracting officer and/or withholding of payments (see 252.244–7001, Contractor Purchasing System Administration).

(b) *System criteria.* A counterfeit electronic part detection and avoidance system shall include risk-based policies and procedures that address, at a minimum, the following areas (see 252.246–7007, Contractor Counterfeit Electronic Part Detection and Avoidance System):

(1) The training of personnel.

(2) The inspection and testing of electronic parts, including criteria for acceptance and rejection.

(3) Processes to abolish counterfeit parts proliferation.

(4) Processes for maintaining electronic part traceability.

(5) 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.

(6) The reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts.

(7) Methodologies to identify suspect counterfeit electronic parts and to rapidly determine if a suspect counterfeit electronic 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) Flow down of counterfeit detection and avoidance requirements.

(10) Process for keeping continually informed of current counterfeiting information and trends.

(11) Process for screening the Government-Industry Data Exchange Program (GIDEP) reports and other credible sources of counterfeiting information.

(12) Control of obsolete electronic parts.

#### 246.870-3 Contract clause.

(a) Except as provided in paragraph (b) of this section, use the clause at 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, in solicitations and contracts when procuring—

(1) Electronic parts;

(2) End items, components, parts, or assemblies containing electronic parts; or

(3) Services where the contractor will supply electronic parts or components, parts, or assemblies containing electronic parts as part of the service.

(b) Do not use the clause in solicitations and contracts that are set-aside for small business.

#### PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

■ 7. Amend section 252.244-7001 by—

■ a. Revising the introductory text, clause title and date;

■ b. Revising paragraphs (c)(19), (20) and (21); and

■ c. Adding Alternate I.

Revised text reads as follows:

#### 252.244-7001 Contractor Purchasing System Administration.

As prescribed in 244.305-71, use one of the following clauses:

*Basic.* As prescribed in 244.305-71(a), use the following clause.

#### CONTRACTOR PURCHASING SYSTEM ADMINISTRATION—BASIC (MAY 2014)

\* \* \* \* \*

(c) \* \* \*

(19) Establish and maintain policies and procedures to ensure purchase orders and subcontracts contain mandatory and applicable flowdown clauses, as required by the FAR and DFARS, including terms and conditions required by the prime contract and any clauses required to carry out the requirements of the prime contract, including the requirements of 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, if applicable;

(20) Provide for an organizational and administrative structure that ensures effective and efficient procurement of required quality materials and parts at the best value from responsible and reliable sources, including the requirements of 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, if applicable;

(21) Establish and maintain selection processes to ensure the most responsive and responsible sources for furnishing required quality parts and materials and to promote competitive sourcing among dependable suppliers so that purchases are reasonably priced and from sources that meet contractor quality requirements, including the requirements of 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, and the item marking requirements of 252.211-7003, Item Unique Identification and Valuation, if applicable;

\* \* \* \* \*

*Alternate I.* As prescribed in 244.305-71(b), use the following clause, which amends paragraph (c) of the basic clause by deleting paragraphs (c)(1) through (c)(18) and (c)(22) through (c)(24), and revising and renumbering paragraphs (c)(19) through (c)(21) of the basic clause.

#### CONTRACTOR PURCHASING SYSTEM ADMINISTRATION—ALTERNATE I (MAY 2014)

The following paragraphs (a) through (f) of this clause do not apply unless the Contractor is subject to the Cost Accounting Standards under 41 U.S.C. chapter 15, as implemented in regulations found at 48 CFR 9903.201-1.

(a) *Definitions.* As used in this clause—

*Acceptable purchasing system* means a purchasing system that complies with the system criteria in paragraph (c) of this clause.

*Purchasing system* means the Contractor's system or systems for purchasing and subcontracting, including make-or-buy decisions, the selection of vendors, analysis of quoted prices, negotiation of prices with vendors, placing and administering of orders, and expediting delivery of materials.

*Significant deficiency* means a shortcoming in the system that materially affects the ability of officials of the Department of Defense to rely upon information produced by the system that is needed for management purposes.

(b) *Acceptable purchasing system.* The Contractor shall establish and maintain an acceptable purchasing system. Failure to maintain an acceptable purchasing system, as defined in this clause, may result in disapproval of the system by the Contracting Officer and/or withholding of payments.

(c) *System criteria.* The Contractor's purchasing system shall—

(1) Establish and maintain policies and procedures to ensure purchase orders and subcontracts contain mandatory and applicable flowdown clauses, as required by the FAR and DFARS, including terms and conditions required by the prime contract and any clauses required to carry out the requirements of the prime contract, including the requirements of 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System;

(2) Provide for an organizational and administrative structure that ensures effective and efficient procurement of required quality materials and parts at the best value from responsible and reliable sources, including the requirements of 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, and, if applicable, the item marking requirements of 252.211-7003, Item Unique Identification and Valuation; and

(3) Establish and maintain selection processes to ensure the most responsive and responsible sources for furnishing required quality parts and materials and to promote competitive sourcing among dependable suppliers so that purchases are from sources that meet contractor quality requirements, including the requirements of 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System.

(d) *Significant deficiencies.* (1) The Contracting Officer will provide notification of initial determination to the Contractor, in writing, of any significant deficiencies. The initial determination will describe the deficiency in sufficient detail to allow the Contractor to understand the deficiency.

(2) The Contractor shall respond within 30 days to a written initial determination from the Contracting Officer that identifies significant deficiencies in the Contractor's purchasing system. If the Contractor disagrees with the initial determination, the Contractor shall state, in writing, its rationale for disagreeing.

(3) The Contracting Officer will evaluate the Contractor's response and notify the Contractor, in writing, of the Contracting Officer's final determination concerning—

(i) Remaining significant deficiencies;

(ii) The adequacy of any proposed or completed corrective action; and

(iii) System disapproval, if the Contracting Officer determines that one or more significant deficiencies remain.

(e) If the Contractor receives the Contracting Officer's final determination of significant deficiencies, the Contractor shall, within 45 days of receipt of the final determination, either correct the significant deficiencies or submit an acceptable corrective action plan showing milestones and actions to eliminate the deficiencies.

(f) *Withholding payments.* If the Contracting Officer makes a final



determination to disapprove the Contractor's purchasing system, and the contract includes the clause at 252.242–7005, Contractor Business Systems, the Contracting Officer will withhold payments in accordance with that clause.

(End of clause)

■ 8. Add new section 252.246–7007 to read as follows:

**252.246–7007 Contractor Counterfeit Electronic Part Detection and Avoidance System.**

As prescribed in 246.870–3, use the following clause:

**CONTRACTOR COUNTERFEIT ELECTRONIC PART DETECTION AND AVOIDANCE SYSTEM (MAY 2014)**

The following paragraphs (a) through (e) of this clause do not apply unless the Contractor is subject to the Cost Accounting Standards under 41 U.S.C. chapter 15, as implemented in regulations found at 48 CFR 9903.201–1.

(a) *Definitions.* As used in this clause—

*Counterfeit electronic part* means an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.

*Electronic part* means an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly (section 818(f)(2) of Pub. L. 112–81). The term “electronic part” includes any embedded software or firmware.

*Obsolete electronic part* means an electronic part that is no longer in production by the original manufacturer or an aftermarket manufacturer that has been provided express written authorization from the current design activity or original manufacturer.

*Suspect counterfeit electronic part* means an electronic part for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic.

(b) *Acceptable counterfeit electronic part detection and avoidance system.* The Contractor shall establish and maintain an acceptable counterfeit electronic part detection and avoidance system. Failure to

maintain an acceptable counterfeit electronic part detection and avoidance system, as defined in this clause, may result in disapproval of the purchasing system by the Contracting Officer and/or withholding of payments.

(c) *System criteria.* A counterfeit electronic part detection and avoidance system shall include risk-based policies and procedures that address, at a minimum, the following areas:

(1) The training of personnel.

(2) The inspection and testing of electronic parts, including criteria for acceptance and rejection. Tests and inspections shall be performed in accordance with accepted Government- and industry-recognized techniques. Selection of tests and inspections shall be based on minimizing risk to the Government. Determination of risk shall be based on the assessed probability of receiving a counterfeit electronic part; the probability that the inspection or test selected will detect a counterfeit electronic part; and 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.

(3) Processes to abolish counterfeit parts proliferation.

(4) Processes for maintaining electronic part traceability (e.g., item unique identification) that enable tracking of the supply chain back to the original manufacturer, whether the electronic parts are supplied as discrete electronic parts or are contained in assemblies. This traceability process shall include certification and traceability documentation developed by manufacturers in accordance with Government and industry standards; clear identification of the name and location of supply chain intermediaries from the manufacturer to the direct source of the product for the seller; and where available, the manufacturer's batch identification for the electronic part(s), such as date codes, lot codes, or serial numbers. If IUID marking is selected as a traceability mechanism, its usage shall comply with the item marking requirements of 252.211–7003, Item Unique Identification and Valuation.

(5) Use of suppliers that are the original manufacturer, or 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. When parts are not available from any of these sources, use of suppliers that meet applicable counterfeit detection and avoidance system criteria.

(6) Reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts. Reporting is required to the Contracting Officer and to the Government-Industry Data Exchange Program

(GIDEP) when the Contractor becomes aware of, or has reason to suspect that, any electronic part or end item, component, part, or assembly containing electronic parts purchased by the DoD, or purchased by a Contractor for delivery to, or on behalf of, the DoD, contains counterfeit electronic parts or suspect counterfeit electronic parts.

Counterfeit electronic parts and suspect counterfeit electronic parts shall not be returned to the seller or otherwise returned to the supply chain until such time that the parts are determined to be authentic.

(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. The Contractor may elect to use current Government- or industry-recognized standards to meet this requirement.

(9) Flowdown of counterfeit detection and avoidance requirements, including applicable system criteria provided herein, to subcontractors 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.

(10) Process for keeping continually informed of current counterfeiting information and trends, including detection and avoidance techniques contained in appropriate industry standards, and using such information and techniques for continuously upgrading internal processes.

(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 in order to maximize the availability and use of authentic, originally designed, and qualified electronic parts throughout the product's life cycle.

(d) Government review and evaluation of the Contractor's policies and procedures will be accomplished as part of the evaluation of the Contractor's purchasing system in accordance with 252.244–7001, Contractor Purchasing System Administration—Basic, or Contractor Purchasing System Administration—Alternate I.

(e) The Contractor shall include the substance of this clause, including paragraphs (a) through (e), in subcontracts, including subcontracts for commercial items, for electronic parts or assemblies containing electronic parts.

(End of clause)

[FR Doc. 2014–10326 Filed 5–5–14; 8:45 am]

**BILLING CODE 5001–06–P**