THOMSON REUTERS

BRIEFING PAPERS® SECOND SERIES

PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

COUNTERFEIT ELECTRONIC PARTS—THE DFARS FINAL RULE AND THE EXPANDED REPORTING REQUIREMENTS FOR NONCONFORMING ITEMS

By Dean P. Vanek and Steven D. Tibbets

In the last several years, an epidemic of counterfeit items—electronic components, in particular—in the supply chains of defense contractors supporting the U.S. Department of Defense (DOD) has led to a great deal of congressional scrutiny. This scrutiny has led to new legislation and implementing regulations intended to eradicate counterfeit items. At the same time, proposed and final regulations designed to enhance federal contractors' conformance to quality standards have been introduced. The new anti-counterfeit and quality standards regulations target contractors providing goods and services to both military and civilian agencies. Thus, developments in this area pose significant new compliance obligations and challenges for a wide swath of federal contractors.

This BRIEFING PAPER presents a comprehensive analysis of legal issues Government contractors face that pertain to counterfeit and nonconforming items. The PAPER covers both longstanding legal rules and principles implicated by counterfeit and nonconforming items, including contract default, false claims, and remediation, and new statutes and regulations intended to enhance the Government's ability to eliminate counterfeit and nonconforming items from its—and its contractors'—supply chains.

IN BRIEF

Dean P. Vanek is a principal of the Chicago-based Law Firm GCL Group, Chartered. Steven D. Tibbets is Counsel with CA Technologies, Inc. in Herndon, Virginia.

Long-Time Sources Of Liability For Counterfeits & Nonconforming Items

While counterfeit parts and nonconforming items have been the subject of recent new regulations, a number of longstanding legal principles and acquisition laws have applied, and will continue to apply, to the introduction of counterfeit parts in contractor supply chains and the sale of nonconforming goods or services to the Government. The following discussion first outlines the legal authorities that impose contractor liability related to counterfeit or nonconforming items, then addresses the remedies available to the Government when issues related to counterfeit or nonconforming items arise.

■ Legal Authorities Imposing Liability Related To Counterfeit Or Nonconforming Items

Broadly, authorities imposing liability for counterfeit or nonconforming items fall into two intuitive categories: (1) authorities that require contract performance to adhere to contract terms; and (2) authorities that impose liability for incorrectly or falsely certifying that items delivered to the Government adhere to contract terms.

(1) *Adhering to Contract Terms*—It is axiomatic that delivering a product that does not conform to a contractual description of the product to be delivered ordinarily constitutes a breach of contract. The Federal Acquisition Regulation (FAR) provides, "Agencies shall ensure that… [s]upplies or services tendered by contractors meet contract requirements."[1] "The Government is entitled to insist on strict compliance, and has no obligation to accept substitutes, even if the substitutes are equivalent or superior to that which is specified."[2] The elements of a claim for breach of a Government contract are the same as for breach of a commercial contract: the "defendant must prove the existence of a contract, performance by the Government, breach by the contractor, and injury to the Government."[3]

In addition to product specifications, the FAR requires contractors to conform to quality standards. For example, where a contractor fails to comply with standard FAR clauses imposing inspection requirements, its goods are "nonconforming" regardless of whether there are any problems with the items themselves, as opposed to whether they have undergone required inspection processes.[4]

When a contractor breaches a Government contract, the Government may be entitled to reimbursement of excess costs associated with defective performance, recovery of overpayments, reductions in contract price caused by defective pricing or failure to comply with Cost Accounting Standards, imposition of a termination for default, or an assessment of liquidated damages.[5]

(2) *Civil and Criminal False Claims*—The civil False Claims Act permits the Government to recover treble damages and penalties from any persons, which includes business entities, who submit false claims for payment to a federal agency.[6] In many cases, furnishing products that do not conform to contract specifications may be interpreted as the presentation of a false claim, particularly where the contractor has made an "implied false certification" by certifying that an item delivered to the Government conformed to all requirements. "Innocent mistakes or negligence in submitting a

THOMSON REUTERS

BRIEFING PAPERS

BRIEFING PAPERS® (ISSN 0007-0025) is published monthly except January (two issues) and copyrighted © 2014 ■ Valerie L. Gross, Editor ■ Periodicals postage paid at St. Paul, MN ■ Published by Thomson Reuters / 610 Opperman Drive, P.O. Box 64526 / St. Paul, MN 55164-0526 ■ http://www.legalsolutions.thomsonreuters.com ■ Customer Service: (800) 328-4880 ■ Postmaster: Send address changes to Briefing Papers / PO Box 64526 / St. Paul, MN 55164-0526

claim are not violations under the [False Claims] Act,"[7] but the False Claims Act imposes liability when a contractor acts with "reckless disregard" as to claims it submits.[8] This "reckless disregard" intent standard has been described as a "very low threshold,"[9] and it means that contractors may incur false claims liability even when they do not intend to submit a false claim and that contractors may not avoid liability by simply ignoring whether the items they furnish to the Government contain counterfeits or otherwise fail to conform to contract specifications. For example, in one case, simply alleging that a contractor sought payment for delivered products that did not conform to a contractually required specification was sufficient to state a claim that the contractor knowingly presented a false claim.[10]

In addition to the civil False Claims Act, there are a number of criminal statutes under which the Government prosecutes procurement fraud, including the criminal False Claims Act,[11] the false statements statue,[12] (3) the mail and wire fraud statutes,[13] (4) the Major Fraud Act of 1988,[14] and (5) criminal health care fraud statutes.[15] Conviction for a criminal offense under these statutes can result in substantial fines and imprisonment.[16]

The criminal False Claims Act makes it a criminal act to present to the Government "any claim upon or against the United States, or any department or agency thereof, knowing such claim to be false fictitious, or fraudulent"[17] "As a practical matter, any invoice or other demand for payment or property from the Government is a 'claim,' and it is probably a 'false claim' if it contains any incorrect or misleading information relating to that demand for payment,"[18] which is essentially the same as under the civil False Claims Act. The "knowing" intent requirement under the criminal False Claims Act, however, requires a greater level of culpability than the intent standard of the civil False Claims Act, under which "reckless disregard" for the truth or falsity of a claim is sufficient to establish liability.[19] Under the criminal False Claims Act, "the Government must prove…that the defendant *knew* the claim was false, fictitious, or fraudulent."[20] A person convicted under the criminal False Claims Act is subject to imprisonment and fines, which can be as high as $1 million per contract.[21]

The false statements statute establishes several criminal offenses, including concealing a material fact, making false statements or false representations, and making false writings.[22] There are five elements to commit an offense under the false statements statute: (1) a statement must be made; (2) the statement must be false; (3) the person making the statement knew it was false, fictitious, or fraudulent when it was made; (4) the statement was material, which means it had a tendency to influence the Government's action or determination (e.g., paying a contractor); and (5) the statement concerned a matter within the jurisdiction of a federal agency.[23] Basically, any false statement that could serve as a basis for liability under the criminal False Claims Act could serve as a basis for liability under the false statements statute, except that the false statements statute criminalizes statements that can influence a Government action or determination, whereas the criminal False Claims Act is limited to false statements that relate to claims for payment.

■ Consequences For Using Counterfeits

(a) *Termination for Default*—A termination for default is one of the most serious negative events a contractor can experience.[24] Not only may the contractor be required to compensate the Government for the extra costs associated with reprocurement, but the contractor's past performance profile will be downgraded and the contractor may face a Government determination that it is not a responsible contractor, which may lead to suspension or debarment.[25]

In terms of mechanics, a contractor's failure to deliver supplies required by the date required under a fixed-price contract immediately provides a basis for the agency to terminate a contract for default.[26] If, however, the Government detects a nonconformity in the contractor's supplies or services 10 or more days before the time set forth in the contract has expired, the Government must provide a "cure notice," i.e., the Government must notify the contractor and give the contractor 10 days to correct the issue.[27] At that point, the Government may terminate the contract for default only if the contractor fails to cure the deficiency within the 10-day period.[28]

While the Government, as mentioned above, is entitled to strict compliance with contract terms and conditions, the principle of "substantial compliance" protects contractors from terminations for default "if the contractor's performance deviates only in minor respects from a contract's requirements."[29] In that situation, a contractor may face some liability for failing to strictly comply with the contract's terms (e.g., an equitable adjustment), but would not face the severe consequences of a termination for default. A 1966 decision of the U.S. Court of Claims, which boards of contract appeals have regularly applied in the decades since, outlined four elements a contractor must establish to avoid termination for default in cases of substantial compliance: (1) supplies must be delivered on time; (2) the supplies must substantially conform to requirements in the contract; (3) the contractor's belief that the supplies conformed to the contract must be reasonable; and (4) the nonconformance must be minor and correctable within a reasonable time.[30]

Although the principle exists in the field of Government contracts, contractors generally should not expect that "substantial performance" will insulate them from terminations for default. "Substantial performance is 'never properly invoked unless the promisee has obtained to all intents and purposes all benefits which he reasonably anticipated receiving under the contract.'"[31] In addition, "default terminations, mostly in older decisions, have been upheld even though the deviations (a) were minor in nature, (b) were otherwise in accordance with commercial practice, and (c) resulted in products as good as or better than the specified ones."[32]

There is a limited exception to the general rule that Government may insist upon strict performance. Agencies may not be permitted to insist on strict performance when the removal of nonconforming, but still adequate, completed work would cause "economic waste."[33] For the most part, though, it is well within agencies' discretion to insist upon strict performance, even when it seems unnecessary and cumbersome from the contractor's perspectives.

(b) *Reprocurement or Remediation*—Following termination of a contract for default, the Government is entitled to "excess costs" or the difference between the contract price of the terminated contract and the price the Government must pay to the reprocurement contractor,[34] though contracts occasionally provide for particular liquidated damages or other damages amounts.[35]

When a contractor furnishes products that have not undergone testing required by a contract, for example, the Government is entitled to remediation in the form of the contractor's conducting the testing (and removing and reinstalling any improperly tested components from finished items). The Government's rights in this context are broad—even where the Government has received some notice that an item contains defects and accepted the item, the Government may claim that the contractor's failure to fully disclose a failure to test constituted fraud and revoke its acceptance of the items, which cuts off the contractor's right to be paid for items it delivered until after remediation is complete.[36]

(c) *Negative Impact on Responsibility and Past Performance and Other Liability*—"Responsibility" refers to a contractor's ability to perform a contract.[37] A contractor that can perform is "responsible," while a contractor that cannot perform is "nonresponsible."[38] Contracting Officers (COs) must determine that a contractor is responsible before making an award to that contractor.[39] To be responsible, contractors must, among other things, have "a satisfactory performance record" and "the necessary organization, experience, accounting and operational controls, and technical skills, or the ability to obtain them (including, as appropriate, such elements as production control procedures, property control systems, quality assurance measures, and safety programs applicable to materials to be produced or services to be performed by the prospective contractor and subcontractors)."[40] Delivering nonconforming or counterfeit items to a Government customer places a contractor at risk that the Government will find that it is nonresponsible under these criteria.

When a contractor is found not to be responsible, it may be suspended (temporarily disqualified from Government contracting during the pendency of an investigation and ensuing legal proceedings) or debarred (excluded from

Government contracting for some specified period).[41] Grounds for debarment set forth in the FAR include, among other things, "[v]iolation of the terms of a Government contract or subcontract so serious as to justify debarment, such as—(A) Willful failure to perform in accordance with the terms of one or more contracts; or (B) A history of failure to perform, or of unsatisfactory performance of, one or more contracts."[42] While it is seldom completely clear whether a particular violation of the terms of a Government contract was "willful," nevertheless, if a contractor establishes a track record of delivering nonconforming or counterfeit items to Government customers, that pattern may establish that noncompliance was willful, which may cause the contractor to be suspended from contracting while the Government investigates the contractor's conduct and ultimately debarred from contracting if the Government finds that the contractor's conduct meets the FAR's debarment criteria.

In addition to responsibility, COs must consider contractors' past performance records when making award decisions.[43] Both agencies and contractors must enter certain past performance information in the Government's Federal Awardee Performance and Integrity Information System (FAPIIS).[44] The FAR expressly provides that information regarding contractors past performance is relevant to award decisions and includes, among other things, contractors' history of "[c]onforming to requirements and to standards of good workmanship," "[a]dherence to schedules, including the administrative aspects of performance," and "[r]reasonable and cooperative behavior and commitment to customer satisfaction."[45] Delivery of nonconforming or counterfeit items will be reflected negatively in a contractor's past performance profile and taken into account by agencies when considering the contractor for awards.

In addition to the Government contract-specific sources of liability, contractors should understand that other bodies of law may assign liability based on the delivery of nonconforming or counterfeit items. For example, if a nonconforming component in a vehicle malfunctions and occupants are hurt or killed, a contractor may face tort-based product liability. Similarly, if a contractor delivers information technology equipment with counterfeit parts containing malware to a Government agency and private information is compromised, for example, the contractor may face liability under privacy laws. It is important for contractors to appreciate that nonconforming and counterfeit items can be sources of both Government contract-specific liability, which this BRIEFING PAPER covers, and other sorts of liability, which are not covered here.

Earlier Government & Industry Efforts To Address Counterfeits & Nonconforming Items

■ Information-Sharing Initiatives

As discussed in detail below, recent statutory and regulatory initiatives to address counterfeit electronic parts include reporting requirements. One goal of such reporting is to ensure that untrustworthy suppliers and counterfeit items are eradicated throughout DOD supply chains in a comprehensive manner and not just from individual contractors' supply chains each time an issue arises. Currently, there are a number of programs and organizations working to serve the same goal. The following discussion highlights several of the leading programs and organizations: (1) Electronic Resellers Association, International, Inc. (ERAI), (2) the Independent Distributors of Electronics Association (IDEA), and (3) the Government Industry Data Exchange Program (GIDEP). Please note that these are only a few of the many sources of information and guidance regarding counterfeit items. Use of resources such as these is a critical part of any counterfeit detection and avoidance program—contractors should be proactive in monitoring their suppliers' industries for counterfeit parts issues.

(1) *ERAI*—ERAI, Inc. describes itself as "a privately held global information services organization that monitors, investigates and reports issues affecting the global electronics supply chain."[46] In 2002, ERAI launched its "High Risk/Suspect Counterfeit Parts" database, which contains the results of ERAI's investigations into counterfeit parts its members have reported and provides a

handy tool for vetting suppliers and electronic items.[47] To take advantage of ERAI's database and other services, a contractor has to be a member of ERAI. Membership requires a financial commitment, but ERAI appears very inclusive and beneficial for contractors in the electronics industry that are willing to pay membership fees. According to its website, "[m]embership in ERAI is available to all companies in the electronics supply chain. ERAI primarily services companies in the defense, aerospace, commercial, medical and nuclear sectors. ERAI's member base ranges from distributors, equipment manufacturers and original component manufacturers to government and enforcement entities."[48]

(2) *IDEA*—IDEA was launched publicly in March 2003. Its objectives are to promote the independent distribution industry through a media advocacy campaign, to improve the quality of products and services through a quality certification program, educational seminars, and conferences, and to promote the study, development, and implementation of techniques and methods designed to improve the business of independent distributors.[49] IDEA offers, among other things, training on avoiding counterfeit electronic parts and has developed quality standards that outline best practices for detecting and avoiding counterfeit items.[50] For example, in October 2006, IDEA released IDEA-STD-1010-A, "Acceptability of Electronic Components Distributed in the Open Market," which furnishes guidance regarding how to inspect items from suppliers for counterfeits.[51]

(3) *GIDEP*—The Government Industry Data Exchange Program, or "GIDEP," "is a cooperative activity between Government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information."[52] Office of Federal Procurement Policy (OFPP) Policy Letter 91-3 designated GIDEP to be the Government's central database for receiving and disseminating information about nonconforming products and materials.[53] Similarly, the DOD has designated GIDEP as the Department's Diminishing Manufacturing Sources and Material Shortages (DMSMS) centralized database for sharing information among industry groups.[54] GIDEP is funded by the U.S. and Canadian Governments. The following types of organizations may become GIDEP members: (1) any U.S. or Canadian industrial organization that supplies items or services (directly or indirectly) to the U.S. Government or to the Canadian Department of Defense, (2) any U.S. or Canadian Government department, agency, or activity; or (3) any licensed U.S. Public Utilities Company.[55]

■ Commercial Industry Standards

There are a number of standards for counterfeit avoidance and detection systems that have been widely accepted as establishing best practices for particular industries. SAE International, for example, has issued two such standards. SAE International describes itself as "a global association of more than 138,000 engineers and related technical experts in the aerospace, automotive and commercial-vehicle industries. SAE International's core competencies are life-long learning and voluntary consensus standards development."[56] SAE has issued a key standard related to counterfeits: AS6081. AS6081 standardizes practices to: identify reliable sources to procure parts; assess and mitigate risk of distributing fraudulent or counterfeit parts; control suspect or confirmed fraudulent or counterfeit parts; and report suspect and confirmed fraudulent or counterfeit parts to other potential users and Government authorities.[57]

The International Organization for Standardization's ISO 9001:2008 standard likewise establishes well-regarded baselines for quality management systems, including detecting and preventing the introduction of counterfeits in companies' supply chains. "ISO 9001:2008 specifies requirements for a quality management system where an organization needs to demonstrate its ability to consistently provide product that meets customer and applicable statutory and regulatory requirements, and aims to enhance customer satisfaction through the effective application of the system, including processes for continual improvement of the system and the assurance of conformity to customer and applicable statutory and regulatory requirements."[58] ISO 9001:2008 is generic and intended to be applicable to all organizations, regardless of the product the organization produces.[59]

Though this PAPER only highlights two illustrative examples here, there are myriad standards on quality and counterfeit avoidance available to contractors, many of which provide guidance specific to particular industries or geographic regions. In addition, some federal contracts are subject to purchasing system, supply inspection, or similar requirements that focus on supply chains.[60] Such requirements are often focused more on obtaining reasonable prices from subcontractors and other vendors than on quality issues, but audits of contractors' systems involve assessing contractors' control over their supply chains. Implementing internal purchasing systems and controls that comply with regulatory guidelines in the FAR and other acquisition regulations is another way contractors can reduce the likelihood that counterfeits will find their way into contractors' supply chains.

The Counterfeit Problem

To say the least, the problem of counterfeit parts in the DOD supply chain is expanding and poses grave danger to the nation's warfighters and the defense operations of the United States. In an effort to address the growing problem of counterfeit parts entering the DOD supply stream, in March 2011 the U.S. Senate Armed Services Committee (SASC) undertook an extensive investigation into the problem of counterfeit electronic parts.[61] The SASC's investigation yielded startling results of the large number of counterfeit parts making their way into the DOD supply chain and into mission critical defense systems. According to the report, the SASC found "a defense supply chain that relies on hundreds of unvetted independent distributors to supply electronic parts for some of [the United States'] most sensitive defense systems" and "overwhelming evidence that companies in China are the primary source of counterfeit electronic parts in the defense supply chain."[62]

Specifically, the SASC investigation concluded that over a two-year period it had identified 1,800 cases of counterfeiting, comprising roughly one million parts.[63] In further support of the Committee's findings, the Department of Commerce reported in 2010 that 9,356 suspected cases of counterfeiting had been identified in the defense industrial supply chain in 2008, which was an almost three-fold increase since 2005.[64]

While counterfeit parts can be found in just about anything, the Committee uncovered numerous examples of suspect counterfeit parts in military systems including on thermal weapon sights for the Army, on mission computers for the Missile Defense Agency's Terminal High Altitude Area Defense (THAAD) missile system, and on military rotary and fixed-wing aircraft ranging from the SH-60B, AH-64, and the CH-46 helicopters to the C-17, C-130J, C-27J, and P-8A Poseidon.[65] So prolific are counterfeit parts that the investigation of the Government Accountability Office (GAO) in support of the SASC found counterfeit parts are readily available on internet purchasing sites.[66]

It is no surprise then that the cost impact of counterfeit electronic parts is significant. Not only do counterfeit parts increase the costs of defense systems, but the cost of remediation to the contractor can be significant, even catastrophic to a business. Reviewing one reported incident, the U.S. Missile Defense Agency discovered computers for the THAAD missile system contained counterfeit memory devices. According to the Missile Defense Agency, the missiles could have failed if the memory devices failed. According to the DOD Director of Operational Test and Evaluation:[67]

> Poor reliability is a problem with major implications for cost….Unreliable systems have higher sustainment costs because…they break more frequently….Poor reliability leads to higher sustainment cost for replacement spares, maintenance, repair parts, facilities, staff, etc. Poor reliability hinders warfighter effectiveness and can essentially render weapons useless.

In the THAAD case, Honeywell, the supplier of the memory devices, purchased the devices from an independent distributor. Honeywell incorporated the devices into mission computers and provided the computers to Lockheed Martin, which in turn delivered the end items to the Missile Defense Agency. Both contractors notified the Government of the suspected counterfeit devices and began fixing the issue. In that case, the Missile Defense Agency actually reimbursed the contractors for approximately $2.7 million in remediation costs, but, as explained in the discussion of contract default and liability above,

such a result is exceptional and contractors are typically liable for remediation costs.[68]

These examples demonstrate how the opportunity to minimize costs pressures—and creates incentives for—contractors to purchase counterfeit supplies. As both military and civilian agencies face tighter budgets and policymakers push for increasing the number of contracts awarded on the basis of the lowest price proposal that is technically acceptable, regardless of the relative quality of competing proposals, conditions are ripe for continued and increasing use of counterfeit items in Government supply chains.

The counterfeit problem is not limited to production-level programs. The problem is exacerbated at the spare, repair, refurbishment, and reset level. The Defense Logistics Agency (DLA) supplies more than 80% of the military's spare parts including electronic parts and components. DLA Land and Marine manages DLA's electronic parts supply chain. When the SASC requested information regarding counterfeit parts from the DLA, the DLA did not maintain a database where actual or suspect counterfeit electronic parts were tracked. Subsequently, the Product Testing Center identified for the Committee 202 cases that involved suspect integrated circuits or discrete devices.[69]

The 202 DLA-identified cases involved 93 separate companies. Thirty-seven of those companies provided suspect parts to the DLA on at least one occasion. Of those 37 companies, more than half provided DLA with suspect parts on three or more occasions.[70]

The suspect counterfeit parts supported hundreds of different weapons systems. According to the DLA's findings, 19 of the 202 parts were used to support more than 100 different weapon systems.[71] One part was found on 176 different weapon systems.[72] Seventy-two of the parts were used on more than 25 weapon systems including the B-52, CH-46 helicopter, F-15 Eagle, C-130J Hercules, the Global Hawk UAV, and the A-10 Thunderbolt. Twenty-six of the suspect parts are used in nuclear reactor programs.[73]

Counterfeit sources are found in many countries. The major source of the counterfeit electronic parts is China, which accounts for 70% of the suspect counterfeit parts reviewed in the SASC investigation originating in China.[74] Perhaps surprisingly, the United Kingdom and Canada have been found to be the second and third major sources, respectively, for counterfeit parts.[75] This can be attributed to the fact that the U.K. and Canada are primary focal points for the distribution and resale of counterfeit parts from China. Also, the close relationship between the U.K. and Canada and the intermingling of sources of supply also contributes to the high incidence of counterfeit supply. However, China is the primary source of the counterfeit problem. The Committee report cited numerous examples of Chinese counterfeit process. For example, e-waste enters the country from Hong Kong. Once in mainland China, e-waste is disassembled, washed in dirty rivers, and dried on sidewalks.[76] Parts are then sanded down and remarked or relabeled. In many cases, manufacturing and date codes are changed to make the parts appear recently manufactured. Then the parts may be recoated and other falsified markings may be placed upon the parts.[77]

FY 2012 NDAA § 818

As a result of the SASC investigation and ensuing report, Congress passed § 818 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012.[78] In addition, § 833 of the FY 2013 NDAA modified, and somewhat expanded upon, § 818 of FY 2012 NDAA.[79] In the following discussion, references to § 818 of FY 2012 NDAA refer to the provision as modified by § 833 of the FY 2013 NDAA.

Section 818 of the FY 2012 NDAA mandates that the Secretary of Defense take certain measures to eliminate counterfeit electronic parts from the DOD supply chain. These steps include, among others, (1) establishing definitions of "counterfeit electronic part" and "suspect counterfeit electronic part," (2) providing guidance for a risk-based approach to prevent their entry into the defense procurement supply chain that addresses training personnel, making sourcing decisions, ensuring traceability of parts, inspecting and testing parts, reporting and quarantining counterfeit and suspect counterfeit electronic

parts, and taking corrective action, and (3) establishing reporting requirements for any actual or suspected counterfeit electronic parts that make their way into the supply chain.[80]

In addition, § 818 requires the DOD to revise the Defense FAR Supplement (DFARS) to address contractor responsibilities for the detection and avoidance of the use of counterfeit electronic parts or suspect counterfeit electronic parts, the use of "trusted suppliers," and reporting counterfeit or suspect counterfeit parts.[81] Section 818 further provides definitions for "electronic parts" the new regulations should cover and "covered contractors" to which the new regulations should apply.[82] "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."[83] Under the definition of "covered contractor," the revised regulations apply only to "CAS-covered" contractors, or contractors performing contracts to which the FAR's Cost Accounting Standards apply.[84]

The DOD also must issue and revise existing guidance for the taking of remedial action against contractors that supply counterfeit electronic parts, or that otherwise fail to detect and avoid their use. COs, by way of example, are now directed to exercise due diligence in the detection and avoidance of such parts and instructed to consider suspending or debarring a supplier until the supplier has effectively remediated the issues leading to the supply of counterfeit electronic parts.[85]

Section 818 further directs the DOD to use the GIDEP reporting system as a means of communicating among DOD personnel the discovery of counterfeit or suspect counterfeit electronic parts in the supply chain. DOD personnel must make a written GIDEP report within 60 days upon discovery or the suspicion of counterfeit electronic parts, and the DOD must establish a process for analyzing and acting upon the reports of counterfeit or suspect counterfeit electronic parts.[86]

Regarding the contractor responsibilities to be implemented in the revised DFARS, § 818 makes covered contractors that supply electronic parts, components, or end items that contain electronic parts responsible for detecting and avoiding the inclusion of such counterfeit or suspect electronic parts into the supply chain.[87] Should counterfeit or suspect counterfeit parts be delivered, the contractor will be held responsible for all rework or corrective action required to remedy the situation. In that case, the cost of the parts themselves and the costs the contractor incurs in the remediation, will be deemed an unallowable cost.[88] Note that the delivery of items containing "suspect counterfeit parts" may trigger remediation obligations regardless of whether the Government can establish that the parts are actually counterfeit.

Moreover, § 818 requires the DOD and its contractors and subcontractors *at all tiers* to develop a trusted supplier supply base.[89] A "trusted supplier" is a supplier selling electronic parts that are currently in production or from stock of the original manufacturer (OEM), the OEM's dealers, or trusted suppliers that obtain such parts exclusively from the OEMs of the parts or their authorized dealers, or, for those parts not currently in production, only from the stock of trusted suppliers.[90] While the definitions and concepts remain the same, the term "trusted suppliers" was dropped from the final rule amending the DFARS to implement § 818.[91]

Section 818 directs the Secretary of Defense to establish requirements for the notification of the DOD and the inspection, testing, and authentication of electronic parts that the Department, its contractors, or subcontractors procure from sources other than a trusted supplier.[92] Those requirements will also consist of a process by which the Department will identify trusted suppliers that have appropriate procedures in place to detect and avoid the introduction of counterfeit or suspect counterfeit parts into the DOD supply chain.[93] Covered contractors must establish a robust set of internal policies and procedures to eliminate counterfeit electronic parts from entering the supply stream.[94] A more complete discussion of contractor internal requirements is found later in this Briefing Paper.

In addition to the DOD's reporting requirements, § 818 requires contractors and

subcontractors to use GIDEP to report counterfeit or suspect counterfeit electronic parts within 60 days of discovery or suspicion.[95] The heretofore voluntary contractor and subcontractor membership of GIDEP now appears to be mandatory. Non-U.S. and non-Canadian suppliers cannot be full members of GIDEP, but they can report using GIDEP and are now obligated under the DFARS rules to do so.

Finally, § 818 the FY 2012 NDAA establishes significant penalties for those committing an intentional offense in trafficking in counterfeit goods or services.[96] Those found to knowingly (a) use a counterfeit mark on or in connection with a good or service, (b) traffic in the labels, patches, or other identifying marks or packaging, or (c) traffic in goods or services knowing that such good or service is a counterfeit military good or service and the use, malfunction, or failure of such counterfeit good or service is likely to cause serious bodily injury or death, impairment of operations, or other significant harm to Government personnel or to national security, shall be fined up to $2 million or imprisoned for up to 10 years or both for the first offense.[97] For corporations and other "persons" other than an individual, fines of up to $5 million may be imposed.[98] For subsequent offences, an individual can be fined up to $5 million or imprisoned for up to 20 years or both, and a corporation can fined up to $15 million.[99]

DFARS Final Rule

On May 6, 2014, the DOD published its final rule revising the DFARS to implement of § 818 of FY 2012 NDAA relating to the detection and avoidance of counterfeit electronic parts.[100] The final rule, which amended DFARS Parts 202, 231, 244, 246, and 252, became effective upon publication.[101] Following publication of the proposed rule in May 2013,[102] the DOD hosted a series of public meetings between the Government and the private sector to solicit the views and opinions of industry, experts, and other interested parties.[103] Since the final rule's publication, public debate, and comment continues regarding the ambiguity and lack of clarity in the final rule.[104]

As discussed above, § 818 of the 2012 NDAA directs the DOD, among other mandates, to create and implement regulations defining (a) counterfeit and suspect counterfeit parts, (b) the responsibilities contractors have to create and implement detection and avoidance systems, and (c) the scope of covered contractors and electronic parts. As part of its effort to meet the NDAA's mandates, the DOD promulgated a new DFARS clause, 252.246-7007, "Contractor Counterfeit Electronic Part Detection and Avoidance System," requiring certain contractors to establish and maintain acceptable counterfeit electronic part detection and avoidance systems. This clause applies to contractors subject to the CAS, including both full and modified CAS coverage.[105]

In addition, the DOD revised the clause at DFARS 252.244-7001, "Contractor Purchasing System Administration," to provide that assessment of counterfeit electronic part detection and avoidance systems is an additional step the Defense Contract Management Agency (DCMA) will complete when performing Contractor Purchasing System Reviews (CPSRs). Failure to maintain acceptable counterfeit electronic part detection and avoidance systems may cause disapproval of contractors' purchasing systems, thereby placing the contractors' eligibility to perform contracts at risk. This DFARS clause applies only to DOD contractors and counterfeit electronic parts and hews closely to § 818's express requirements.[106]

As prescribed in DFARS 246.870-3, the new clause at DFARS 252.246-7007 will be included in all solicitations and contracts 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 services provided.[107] The sole exception to the clause's inclusion is for solicitations and contracts designated as small business set-asides.[108]

The DFARS final rule is limited to electronic parts. Prior to its publication, there was much debate and speculation that the DOD would expand the regulations beyond electronic parts and components. Such an expansion would have exceeded the mandate set forth in § 818 of the FY 2012 NDAA. As discussed below, the FAR Council has introduced a proposed rule that will expand the reporting requirements for all nonconforming

goods.[109] Once final, the proposed FAR rule will extend to all counterfeit and suspect counterfeit materials and nonconforming goods.

■ Key Definitions

The DFARS final rule defines "*counterfeit electronic part*" as:[110]

> [A]n 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. The term "electronic part" includes "any embedded software or firmware."[111] "*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."[112] "*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."[113]

■ Counterfeit Electronic Part

The final rule definition takes into account current industry and agency definitions.[114] Between publication of an initial proposed rule and the final rule on counterfeit electronic parts, the DOD made changes to the definition to align it with the best features of those industry and agency definitions.[115] Nonetheless, the DOD determined that given the lack of uniformity and the inconsistencies in the various industry definitions, it was not feasible to include any one industry definition in its entirety as the DFARS definition.[116]

In order to violate the final rule by supplying "counterfeit electronic parts," a contractor must have the required intent. The use of the term "misrepresented" in the definition of counterfeit electronic part means the contractor or subcontractor must intend to misrepresent the electronic part as authentic and from the original manufacturer or its authorized representative.[117]

Similarly, *scienter* is an element expressed in the counterfeit electronic parts definition. A part that is an unauthorized reproduction, substitution, or alternation must have been "knowingly" mismarked, misidentified, or otherwise misrepresented by the contractor or a subcontractor to be a "counterfeit electronic part" covered by the final rule.[118] Conversely, the definition does not include nor contemplate the concepts of negligence or recklessness in the contractor's failure to identify a counterfeit electronic part before it entered the supply stream, the rationale being that a contractor's negligence or recklessness in maintaining an appropriate detection and avoidance system is not *ipso facto* indicia that the part itself is counterfeit.[119] Keep in mind, however, the point made above that delivery of items containing counterfeit parts may cause a contractor to be in default under a contract, regardless of whether the contractor acts with the intent required to meet the final rule's definition of "counterfeit electronic part."

The counterfeit electronic parts definition defines [un]lawful or unauthorized substitution." A used part represented as new, or the false identification of grade, serial or lot number, date code, or performance characteristics are all evidence of "unlawful or unauthorized substitution."[120] Contractors that supply used or obsolete parts while representing them as new are violating the regulation. Used parts were identified by the SASC as a major concern and a significant contributing source of counterfeit parts in the supply chain.[121]

■ Suspect Counterfeit Part

A "suspect counterfeit part" means an electronic part for which credible evidence provides reasonable doubt for the contractor that the electronic part is authentic.[122] The final rule does not define what "credible evidence" means—and the term is not clearly defined in the FAR even

though it appears in several places, most notably FAR Part 3's "mandatory disclosure rule"[123]—but contractors generally understand the term to mean that company management has received some information indicating that a counterfeit item has been detected in the contractor's supply chain and the information appears to be valid following a limited preliminary investigation.[124] In the preamble to the final rule, however, the DOD states that, as with all nonconforming items, the CO is responsible for acceptance under the FAR.[125] The final rule requires the contractor to determine a part's authenticity through a number of means including, but not limited to, testing and inspection. It is clear from the preamble that the DOD recognizes it may be impracticable and not cost effective for a contractor to test each suspect part. Therefore, a fact-based, case-by-case approach to testing and inspecting different parts by the contractor is warranted.[126]

■ Obsolete Electronic Part

A supplier may provide to the Government an electronic part that is no longer in production by the OEM. However, that electronic part must have been manufactured by an aftermarket manufacturer that has the *express written authorization* from the OEM or the current design activity.[127] Electronic parts supplied by authorized resellers and distributors are also permissible provided that the contractor has the same OEM authorization in writing.[128] Conversely, "obsolete parts" are defined as electronic parts that are not supplied by the OEM or an aftermarket manufacturer authorized by the design activity or the OEM.[129] Obsolete parts are an "unauthorized substitution" as contained in the definition of "counterfeit electronic part."[130]

From where, and from whom, may electronic parts be supplied? Consistent with FY 2012 NDAA § 818, the DOD and its contractors and subcontractors must, whenever possible, supply electronic parts that are currently in production or in stock from the OEM or an OEM-authorized dealer.[131] As stated above, where the electronic part is no longer in production, contractors may supply compliant electronic parts from those suppliers the OEM or current design activity has expressly authorized in writing to supply the parts.[132]

Where electronic parts are no longer available from any of those sources, as a final alternative, electronic parts may be supplied by suppliers that have in place demonstrable and acceptable counterfeit detection and avoidance systems.[133]

■ System Criteria

As a result of the final rule, contractors that are subject to the CAS and their subcontractors that supply electronic parts to the Government are now required to implement acceptable counterfeit detection and avoidance systems. Contractors and subcontractors that fail to do so are subject to disapproval of their purchasing systems and withholding of contract payments.[134] The "Contractor Counterfeit Electronic Part Detection and Avoidance System" clause at DFARS 252.246-7007 added by the final rule identifies 12 areas that "*at a minimum*," each CAS covered contractor's counterfeit detection and avoidance system must address:[135]

> (1) The training of personnel.
>
> (2) The inspection and testing of electronic parts, including criteria for acceptance and rejection. Tests and inspection 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) [A] process for maintaining electronic part traceability (e.g., item unique identification) that enable[s] 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 of 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 [DFARS] 252.211-7003, Item Unique Identification and Validation.

(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 parts. Reporting is required to the Contracting Officer and to [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 electronic 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.

A contractor's counterfeit detection and avoidance system must be premised on a risk-based approach.[136] Each contractor must assess the risks inherent in its operations and supply chain based on the potential for receipt of counterfeit parts from different sources. Contractors must assess their downstream supply chains, identify the risks inherent in their supply streams, revise internal procedures capturing the minimum criteria set forth above, audit their supply bases, test and inspect incoming electronic parts using procedures appropriate in light of the risks presented by a source, provide the appropriate level of training to its employees, and continually monitor the effectiveness of its detection and avoidance system. While CAS-covered contractors currently undergo stringent evaluation and approval of six major business systems,[137] having an effective counterfeit detection and avoidance system is not a part of this list of critical business systems and, therefore, represents a compliance obligation above and beyond prior business system requirements.

The review and approval of a contractor's internal policies, procedures, and system criteria will be accomplished by the Government through the DFARS Subpart 244.3, "Contractor Purchasing System Review" process.[138] The DCMA has developed a counterfeit detection and avoidance system checklist for use in the CPSR reviews.[139] Contractors must be aware that failure to maintain an acceptable system for the detection and avoidance of counterfeit parts can result in failure of the CPSR review and the potential withholding of contract payments.[140]

■ Traceability

A key component to an effective counterfeit detection and avoidance system is electronic part traceability. The DFARS final rule requires that a contractor's system include certification and traceability documentation.[141] The final rule does not express nor mandate specific technology to be used for traceability purposes. The silence in the final rule is intended to provide contractors with flexibility in determining which industry standards and best practices are most suitable for a contractor's risk-based approach.[142]

Item unique identification (IUID), which is referenced in the new DFARS 252.246-7007

clause,[143] is the optimal technique for achieving traceability.[144] Currently, the "Item Unique Identification and Valuation "clause at DFARS 252.211-7003 requires IUID for acquisitions of $5,000 or more. The DOD may request the use of IUID in lower value acquisitions in the event the item being acquired is critical material susceptible to counterfeiting and is "mission essential" or "controlled inventory." In addition, regardless of acquisition value, the DOD may require IUID for a serially managed item, or a subassembly, component, or part of a serially managed item, a warranted serialized item, an item that involves special tooling or test equipment for a major defense acquisition program, or an item that has otherwise been identified by the procuring agency as vulnerable to supply chain threats.[145]

Electronic parts manufactured and in inventory and not procured under a prior contract will be subject to the same rules as electronic parts manufactured post contract award. For mission critical electronic parts and components that could impact human life, the DOD maintains a "zero tolerance" policy for counterfeits.[146]

■ Reporting & Quarantining

Contractors must identify and remove from their production processes any counterfeit or suspect counterfeit electronic parts. With respect to suspect counterfeit parts, contractors are expected to timely determine whether or not a part is indeed counterfeit.[147] While the final rule does not mandate a process for such determinations, contractors are expected to employ industry standards and best practices in the determination process.[148] Once determined, counterfeit parts are to be removed and quarantined until disposition instructions are received.[149]

Finally, as mentioned above, contractors and COs must report counterfeit or suspect counterfeit parts to the CO through GIDEP.[150]

■ Commercial Items

The final rule does not apply to prime contracts for the acquisition of commercial items. The exclusion includes commercial off-the-shelf items (COTS) items.[151] Because the CAS do not apply to commercial items,[152] most contractors supplying commercial items are not CAS covered. However, the Director, Defense Procurement and Acquisition Policy (DPAP), has determined that DFARS 252.246-7007 does apply to *subcontracts* for commercial and COTS items.[153] The clause provides that prime contractors "shall include the *substance* of the clause including paragraphs (a) through (e) in subcontracts including subcontracts for the supply of commercial items."[154] What is precisely intended by the final rule's use of the "substance of this clause" and what discretion it confers on prime contractors, is unclear. As mentioned above, the final rule contains a mandatory flowdown requirement to all subcontractors.[155] Therefore, suppliers of commercial items to CAS-covered prime contractors should expect their customers will seek to require such subcontractors to adopt counterfeit avoidance and detection measures required by the final rule.

Section 818 of the FY 2012 NDAA did not specifically address the exemption or application of a counterfeit detection and avoidance system to commercial item procurements. As noted in the preamble to the final rule, the provisions of § 818 requiring implementation of a contract clause meet the criteria set forth in 41 U.S.C.A. §§ 1906 and 1907.[156] Consequently, unless the Director of DPAP makes a written determination that it is not in the best interest of the Government to exempt contracts and subcontracts for the acquisition of commercial items, the final rule will not apply at the prime level for the acquisition of commercial and COTS items. The Director DPAP did, however, determine that the final rule *is* applicable to subcontracts for the acquisition of commercial and COTS electronic parts.[157]

The paradoxical result is that CAS-covered prime contractors procuring commercial or COTS electronic parts from a sub-tier suppliers must include the restrictions concerning counterfeit and suspect counterfeit parts in their subcontracts. The flowdown requirement is mandatory for all levels of the supply chain.[158]

FAR Case 2013-002 Expanded Reporting Of Nonconforming Items

On June 10, 2014, the Federal Acquisition Regulation Council issued a proposed rule in

FAR Case 2013-002, "Expanded Reporting of Nonconforming Items."[159] As discussed above, while counterfeit electronic parts have received a great deal of attention from Congress and regulators, the FAR proposed rule would extend counterfeit regulations beyond simply electronic parts to other types of items and materials.[160]

Under the proposed rule, virtually all contractors, including commercial item and small business contractors, would be required to report counterfeit and nonconforming items and materials they find in their supply chains when those items could lead to certain types of harm. As stated in the proposed rule's preamble, "the problem of counterfeit and nonconforming parts extends far beyond electronic parts and can impact the mission of all Government agencies."[161] Thus, the FAR Council determined that FY 2012 NDAA § 818 provides the backdrop to expand the requirements beyond electronic parts.[162]

Eighteen comments in response to the proposed rule were submitted to the FAR Council by the public comment closing date of September 10, 2014.[163] On September 29, 2014, the Defense Acquisition Regulations Council Director appointed an ad hoc committee to review the public comments in response to the proposed rule and to draft the final rule. The final report on the proposed rule is now slated for November 19, 2014.[164]

The FAR Council determined that the previously discussed DFARS rule was not, by itself, sufficient to address the problem of counterfeit parts. "While section 818 applied only to DOD, only to electronic products, and only to contractors covered by the [CAS], the FAR Council concluded that the principles expressed in section 818 should be applied beyond DOD, should not be limited to electronic products, and should not be limited to CAS-covered contractors."[165] Furthermore, while OFPP Policy Letter 91-3 requires *agencies* to report to GIDEP, the FAR Council believes that the timeliness and effectiveness of the reporting will be enhanced if *contractors* report directly to GIDEP.[166]

Like the DFARS final rule, the FAR proposed rule is intended to mitigate the growing threat to an agency's mission and vital systems that counterfeit items in a global supply chain pose. Accordingly, the proposed rule would reduce the risks by ensuring that contractors timely report suspect items in a widely available database. The proposed rule would extend counterfeit prevention efforts beyond counterfeit electronic parts and beyond CAS-covered DOD contractors to all suppliers providing goods or services to the Government.[167]

■ Key Definitions

The proposed rule defines certain key terms. For use exclusively in FAR Part 46, "Quality Assurance, it defines "common item" to mean "an item that has multiple applications versus a single or peculiar application. Common items include, for example, raw or processed materials, parts, components, subassemblies, and finished assemblies that are commonly available products (such as nondevelopmental items, off-the-shelf items, National Stock Number items, or commercial catalog items)."[168] The phrase "counterfeit item" refers to "an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified item from the original manufacturer, or a source with the express written authority of the original manufacturer or design activity, including an authorized aftermarket manufacturer."[169] "Quality escape" refers to "a situation in which a supplier's internal quality control system fails to identify and contain a nonconforming condition."[170]

A "suspect counterfeit item" is "an item for which credible evidence (including but not limited, visual inspection or testing) provides reasonable doubt that the item is authentic."[171] The FAR Council noted that "critical nonconformance" is already defined at FAR 46.101 as a nonconformance that is likely to result in hazardous or unsafe conditions for individuals using, maintaining, or depending on the supplies or services or that is likely to prevent performance of a vital agency mission. Likewise, "major nonconformance" also is already defined at FAR 46.101 as a nonconformance that is not critical, but is likely to result in failure of the supplies or services or to materially reduce the usability of the supplies or services for their intended purpose.[172]

■ Scope

The proposed rule would add a number of requirements to any contract for supplies that are (a) delivered to the Government, (b) acquired by the contractor for use in performing services, or (c) furnished by the contractor for use by or for the Government.[173]

The proposed rule would require COs to describe during acquisition planning how they plan to administer a contract with respect to inspection and acceptance (for services) and with respect to the risk-based Government quality assurance measures used to identify and control major and critical nonconformances, including use of GIDEP (for supplies).[174] In addition to imposing this obligation on COs, the proposed rule provides that any contractor performing a contract involving supplies (including contracts that mainly involve services, but also that include some ancillary supplies), must use GIDEP to report counterfeits or suspected counterfeits as explained in more detail below.[175]

The proposed rule includes ensuring that vendors or suppliers of raw or processed materials, parts, components, subassemblies, and finished assemblies have acceptable quality control systems in a list of "contractor responsibilities," but the rule does not explain exactly what contractors must do to monitor or verify their suppliers' quality control systems.[176] Contractors must further ensure that any quality escapes of their vendors are not incorporated into the contractors' products.[177]

The proposed rule is intended to build on a contractor's current quality and inspection system, and it demonstrates the link between a supplier's quality control system and preventing quality escapes from being incorporated into the supply chain. While the FAR Council recognizes that even the best quality system will fail to detect a small percentage of nonconformances, it also stated that ensuring that quality and inspection systems work as well as they possibly can is the "pivotal issue justifying mandatory GIDEP reporting."[178]

■ Reporting

Like the DFARS final rule, the FAR proposed rule would require contractors to monitor or "screen" GIDEP for any counterfeits that other manufacturers have reported and that might affect the contractors' products. In addition, contractors must make certain reports related to counterfeit items, including:

(1) reports to COs within 30 days after a contractor becomes aware that any end item, component, subassembly, part, or material contained in supplies purchased by the contractor for delivery to or for the Government is counterfeit or suspect counterfeit (contractors that make these reports and have the items in their possession must retain the items until they receive disposition instructions from the Government); and

(2) reports to GIDEP within 60 days after the contractor becomes aware that an item purchased by or for the contractor for delivery to or for the Government is counterfeit or suspect counterfeit or contains a major or critical nonconformance that is a common item and constitutes a quality escape that has resulted in the release of like nonconforming items to more than one customer.[179]

The proposed rule will add a new clause at 52.246-XX, "Reporting Nonconforming Items," which must be included in solicitations and contracts for the acquisition of supplies or services that include supplies and that are (a) delivered to the Government, (b) acquired by the contractor for use in performing services, or (c) furnished by the contractor for use by or for the Government. The clause will allow the CO to modify paragraph (c), but only to shift responsibility for GIDEP reporting from the contractor to the CO.[180]

There is a key distinction between circumstances requiring reporting to a CO and circumstances requiring reporting to GIDEP. The CO need not be notified if the contractor identifies a major or critical nonconformance and rectifies the nonconformance prior to delivery. Conversely, the CO *must* be notified if a counterfeit or suspect counterfeit item is identified, regardless of whether the contract rectifies the nonconformance prior to delivery.[181]

Following notification, the CO will provide disposition instructions for the counterfeit or suspect counterfeit item. In some cases, agency policy will require the CO to instruct the contractor's retention of the counterfeit or suspect counterfeit item for investigative or evidentiary purposes.[182]

To summarize the new reporting requirements, the proposed rule contains several conditions that must exist that mandate a GIDEP report: an item (1) must be a counterfeit or suspect counterfeit item, or (2) contain a major or critical nonconformance that is a common item, and (3) that constitutes a quality escape from a lower-level subcontractor or supplier, which (4) results in the release of nonconforming items to more than one customer.[183]

■ Limited Safe Harbor

The proposed rule would implement one "safe harbor" for the DOD contractors that make nonconformance reports for electronic components. For DOD contracts, contractors or subcontractors that provide written reports or notifications under the proposed rule's new contract clause would not be subject to "civil liability on the basis of such reporting, provided that the contractors or subcontractors made a reasonable effort to determine that the end item, component, part, or material contained electronic parts that were counterfeit items or suspect counterfeit items."[184] In other words, contractors subject to the DFARS rule would not face civil liability when they acknowledge counterfeits in their supply chains by submitting nonconforming item reports under the proposed rule.

At least one commenter to the proposed rule posits that while the proposed rule extends beyond counterfeit electronic parts, the limited safe harbor provided for in NDAA § 818 does not extend beyond DOD contractors.[185] Thus a gap is created between the implementation of the DFARS final rule and any future implementation of the proposed rule in its current form. Consequently, there is the real risk that non-DOD contractors that file a good faith report will not be covered by the safe harbor and therefore, a disincentive for contractors to self-report.

■ Flowdown

Like the final rule the proposed rule's contract clause would be required in "all subcontracts for supplies, or services that include supplies, at any tier."[186] Contractors would be responsible for ensuring that vendors and suppliers of raw or processed materials, parts, components, subassemblies, and finished assemblies have an acceptable quality control system to prevent quality escapes at the vendor or supplier tier from being incorporated into the contractor's final product.[187]

■ Commercial Item Acquisitions

The proposed rule would amend FAR 12.208 addressing contract quality assurance in commercial item acquisitions to add a sentence at the end of the paragraph stating that for supply contracts and service contracts that include supplies, contractors shall be required to use GIDEP.[188]

■ Impact On Contractors

In the preamble to the proposed rule, the FAR Council took pains to provide a thorough rationale for extending the proposed rule to cover more contractors and more than just electronic parts, despite § 818's limits.[189] If finalized in its current form contractors selling any tangible items to the Government should take note of the proposed rule, consider whether their products contain "common items" that could lead to "critical" or "major" nonconformances, and begin to assess what procedures and training they will need to implement to comply with new FAR provisions that reflect the proposed rule.

Conclusion

As first codified in the 2012 SASC report, the existence of counterfeit parts in the DOD supply chain is prolific with the threat ever increasing as time passes. Counterfeit parts pose a substantial threat to the warfighter and the national security of the country. The DFARS final rule attempts to ameliorate that treat by mandating that CAS-covered contractors and their suppliers of electronic parts, including commercial and COTS items, institute substantial internal procedures

to detect and avoid the use and supply of counterfeit electronic parts. Like the impact to the warfighter, the impact to contractors for failing to do so can be dramatic and even fatal. While formulating a minimum compliance standard, the new system criteria can dovetail off of existing industry standards and best practices thus reducing the cost impact to contractors and the time required to become compliant.

While commenters can debate whether the FAR Council has statutory or legislative authority to expand the counterfeit rules to all contractors supplying goods and services to any Government agency, the expanded reporting requirements under FAR Case 2013-002 will have a dramatic impact on all contractors of any size and at any tier. What is clear is that contractors supplying electronic parts need to implement detection and avoidance systems that at a minimum comply with the new requirements of the clause at DFARS 252.246-7007. Similarly, contractors of any size and at any tier must begin to assess their internal processes and procedures in an effort to mitigate risk to the supply chain through reporting and notification in contemplation of the publication of a final rule consistent with the FAR Council's current proposed rule.

GUIDELINES

These *Guidelines* are intended to assist you in understanding the legal issues Government contractors face related to counterfeit and nonconforming items. They are not, however, a substitute for professional representation in any particular situation.

1. Firms supplying electronic parts, or items containing electronic parts, used in products purchased by the DOD should assume that their CAS-covered customers will flow down the DFARS clause required by the final rule and assess their ability to implement counterfeit detection and avoidance programs. An honest assessment may reveal that subcontractor firms should simply exit the market or, conversely, may reveal an opportunity to extract premiums from customers where competitors are incapable of implementing counterfeit avoidance and detection systems.

2. Recognize that the current regulatory environment is fluid. All federal contractors and their suppliers should consider how they would react in the event that requirements similar to those in the final DFARs rule are extended to non-DOD procurements and to items beyond electronic parts.

3. Suppliers of electronic parts, or items that contain them, should carefully review their supply base and identify situations in which OEMs or current design activity-approved suppliers are likely to discontinue critical components and determine a strategy for filling future orders of spare parts. Again, there is risk associated with the disappearance of "trusted suppliers" for certain items, but opportunity for those firms that anticipate and exploit the limited number of DFARS-permitted sources for obsolete items.

4. Suppliers of electronic parts, or items that contain them, must assess their internal processes and determine best practices applicable to the specific goods or services the supplier introduces into the supply chain. This includes assessing and developing an adequate inspection, testing, and reporting methodology tailored to the specific goods or services supplied to the Government. There are many existing tools, methodologies, and best practices existing in industry that may not require contractors to reinvent the wheel. Contractors should look to those existing tools, methodologies, and best practices to determine their usefulness in developing an adequate testing, inspection, and reporting process tailored to a contractor's particular goods or services.

5. Suppliers need to develop a robust process for quarantining and destroying counterfeit or suspect counterfeit electronic parts in a manner that ensures the parts or components will not be reintroduced into the supply chain. This includes providing adequate training to employees in the purchasing, quality, inspection, and audit functions on identification of actual or suspect counterfeit electronic parts. Once counterfeit electronic parts are discovered or suspected, contractors must now report their findings in GIDEP.

6. Update existing business systems to include an adequate counterfeit detection and avoidance plan employing risk-based methodologies, and implement the counterfeit detection and avoidance system as part of the contractor's overall purchasing system in a manner adequate to sustain CPSR requirements. An adequate detection and avoidance system must, at a minimum, address the 12 system criteria set forth in the final rule. Contractors must now recognize that an adequate counterfeit detection and avoidance system is an addition to the six existing DFARS-mandated contractor business systems and that the failure to maintain an adequate counterfeit detection and avoidance system runs the risk of withholding contract payments, suspension, debarment, or worse.

★ REFERENCES ★

1/ FAR 46.102(b).

2/ Carothers Constr. Co., ASBCA No. 41268, 93-2 BCA ¶ 25,628.

3/ BMY-Combat Sys. Div. of Harsco Corp. v. United States, 38 Fed. Cl. 109, 127 (1997).

4/ Calif. Aero Dynamics Corp., ASBCA No. 39295, 92-2 BCA ¶ 24,868 (contractor failed to comply with FAR 52.246-2, "Inspection of Supplies—Fixed-Price").

5/ Feldman, Government Contract Guidebook § 22:2 (4th ed. 2012).

6/ 31 U.S.C.A. § 3729.

7/ Feldman, Government Contract Guidebook § 12:4 (4th ed. 2012).

8/ 31 U.S.C.A. § 3729(b)(1)(a)(iii).

9/ Shaw, Wagner & Nichols, "Contractor Responsibility: Toward An Integrated Approach To Legal Risk Management," Briefing Papers No. 13-4, at 3 (Mar. 2013).

10/ United States v. Boeing Co., No. 02-193-AS, 2007 WL 473757, at *4–5 (D. Or. Feb. 5, 2007) (refusing to dismiss False Claims Act claim because allegation that plaintiff sold nonconforming item to Government knowing that it was nonconforming was sufficient to plead the claim even under heightened pleading standard for fraud). Since this decision and others like it were issued, Congress passed the Fraud Enforcement and Recovery Act of 2009, Pub. L. No. 111-21 (2009), which expanded the scope of conduct actionable under the False Claims Act. See Laemmle-Weidenfeld & Schaengold, "Feature Comment: The Impact of the Fraud Enforcement and Recovery Act of 2009 on the Civil False Claims Act," 51 GC ¶ 224 (July 8, 2009); Briggerman, "False Claims Act Amendments: A Major Expansion in the Scope of the Act," 23 Nash & Cibinic Rep. ¶ 58 (Nov. 2009); Branca & Thompson, "Federal False Claims Act 'Corrected and Clarified' To Expand Contractor Liability," Construct!: The Newsletter of the Construction Litigation Committee of the American Bar Association's Section of Litigation (Summer 2009).

11/ 18 U.S.C.A. § 287.

12/ 18 U.S.C.A. § 1001.

13/ 18 U.S.C.A. § 1031.

14/ 18 U.S.C.A. §§ 1341 (mail fraud), 1343 (wire fraud).

15/ E.g., 18 U.S.C.A. § 1347.

16/ See Feldman, Government Contract Guidebook § 12:14 (4th ed. 2012); Goddard, Business Ethics in Government Contracting–Part II, Briefing Papers No. 03-7 (June 2003).

17/ 18 U.S.C.A. § 287.

18/ Feldman, Government Contract Guidebook § 12:16 (4th ed. 2012).

19/ 31 U.S.C.A. § 3729(b)(1)(a)(iii).

20/ Feldman, Government Contract Guidebook § 12:17 (4th ed. 2012).

21/ 18 U.S.C.A. § 287; see Feldman, Government Contract Guidebook § 12:19 (4th ed. 2012).

22/ 18 U.S.C.A. § 1001(a); see Feldman, Government Contract Guidebook § 12:21 (4th ed. 2012).

23/ 18 U.S.C.A. § 1001.

24/ Feldman, Government Contract Guidebook § 19:1 (4th ed. 2012). ("Besides a criminal conviction or debarment or suspension, termination for default is undoubtedly the most severe agency sanction that can befall a Government contractor.").

25/ See FAR subpt. 9.4.

26/ FAR 52.249-8(a)(1)(i). The FAR imposes somewhat different termination terms for commercial item or cost-reimbursement contracts, but they generally require the Government to provide an opportunity to cure deficiencies when the delivery schedule allows. See FAR 12.403(c)(1).

27/ FAR 52.249-8(a)(2).

28/ FAR 52.249-8(a)(2).

29/ Feldman, Government Contract Guidebook § 13:12 (4th ed. 2012).

30/ Feldman, Government Contract Guidebook § 13:14 (4th ed. 2012) (discussing Radiation Tech., Inc. v. United States, 366 F.2d 1003 (Ct. Cl. 1966)).

31/ PCL Constr. Servs., Inc. v. United States, 47 Fed. Cl. 745, 810 (2000) (quoting Blinderman Constr. Co. v. United States, 39 Fed. Cl. 529, 572 (1997)).

32/ Feldman, Government Contract Guidebook § 19:6 (4th ed. 2012).

33/ Granite Const. Co. v. United States, 962 F.2d 998 (Fed. Cir. 1992), 34 GC ¶ 293; see Feldman, Government Contract Guidebook § 13:10 (4th ed. 2012); Cibinic, "Economic Waste: When 'Just As Good' Is Good Enough," 6 Nash & Cibinic Rep. ¶ 28 (May 1992).

34/ FAR 52.249-8(b).

35/ FAR 49.402-7; see FAR subpt. 11.5, 52.211-11 (liquidated damages); Feldman, Government Contract Guidebook § 19:21 (4th ed. 2012).

36/ See BMY-Combat Sys. Div. of Harsco Corp. v. United States, 38 Fed. Cl. 109, 119 (1997) (Government revocation of acceptance was proper where observation and inspection of items would not reveal the failure to conduct required tests). In terms of strategy, this case illustrates how a contractor's seeking an equitable adjustment to recover costs associated with post-acceptance remediation can backfire if the Government asserts counterclaims of fraud and False Claims Act violations. Thus, while it is true that, as discussed above, legal authorities place limits on the Government's ability to force contractors to correct immaterial deficiencies and acceptance of an item may "cut off" the Government's discretion to insist on strict compliance with every term or condition, contractors may often find that the costs and benefits of acquiescing to Government demands are more favorable than the costs and benefits of bringing a claim.

37/ FAR 9.103.

38/ FAR 9.104-1.

39/ FAR 9.103(b).

40/ FAR 9.104-1(c), (e).

41/ See FAR subpt. 9.4. See generally Shaw, Wagner & Nichols, "Contractor Responsibility: Toward An Integrated Approach To Legal Risk Management," Briefing Papers No. 13-4 (Mar. 2013); West, Hatch, Brennan & VanDyke, "Suspension & Debarment," Briefing Papers No. 06-9 (Aug. 2006).

42/ FAR 9.406-2(b)(1)(i).

43/ FAR 15.304(c)(3)(i).

44/ FAR 42.1501.

45/ FAR 42.1501(a).

46/ See http://www.erai.com/aboutus_profile.

47/ See http://www.erai.com/ca_Awareness_Timeline_.

48/ See http://www.erai.com/membership_options_erai_member.

49/ See http://www.idofea.org/about.

50/ See http://www.idofea.org/training.

51/ See http://www.idofea.org/training.

52/ See http://www.gidep.org.

53/ OFPP Policy Letter 91-3 (Apr. 9, 1991), available at http://www.whitehouse.gov/omb/procurement_policy_letter_91-3.

54/ See http://www.gidep.org/data/dmsms/dmsms.htm.

55/ See http://www.gidep.org/about/about.htm.

56/ See http://www.sae.org/about/.

57/ See http://standards.sae.org/as6081/.

58/ See http://www.iso.org/iso/catalogue_detail?csnumber=46486.

59/ See http://www.iso.org/iso/catalogue_detail?csnumber=46486.

60/ E.g., FAR subpt. 44.3, 52.246-1.

61/ S. Comm. on Armed Services, Inquiry Into Counterfeit Electronic Parts in the Department of Defense Supply Chain, S. Rep. No. 112-167 (May 21, 2012), available at https://www.congress.gov/112/crpt/srpt167/CRPT-112srpt167.pdf.

62/ S. Rep. No. 112-167, at i.

63/ S. Rep. No. 112-167, at i–ii.

64/ S. Rep. No. 112-167, at 1 (citing U.S. Department of Commerce, Bureau of Industry and Security, Office of Technical Evaluation Defense Industrial Base Assessment: Counterfeit Electronics i–ii (Jan. 2010), available at http://www.bis.doc.gov/index.php/forms-documents/doc_view/37-defense-industrial-base-assessment-of-counterfeit-electronics-2010).

65/ S. Rep. No. 112-167, at ii.

66/ GAO, DOD Supply Chain: Suspect Counterfeit Electronic Parts Can Be Found on Internet Purchasing Platform, GAO-12-375 (Feb. 12, 2012).

67/ S. Rep. No. 112-167, at 58.

68/ S. Rep. No. 112-167, at 58.

69/ S. Rep. No. 112-167, at 61–62.

70/ S. Rep. No. 112-167, at 62.

71/ S. Rep. No. 112-167, at 63.

72/ S. Rep. No. 112-167, at 63.

73/ S. Rep. No. 112-167, at 63.

74/ S. Rep. No. 112-167, at ii.

75/ S. Rep. No. 112-167, at vi.

76/ S. Rep. No. 112-167, at 6.

77/ S. Rep. No. 112-167, at 6.

78/ National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 818, 125 Stat. 1298, 1493 (2011).

79/ National Defense Authorization Act for Fiscal Year 2013, Pub. L. No. 112-239, § 833, 126 Stat. 1632, 1844 (2013).

80/ Pub. L. No. 112-81, § 818(b).

81/ Pub. L. No. 112-81, § 818(c).

82/ Pub. L. No. 112-81, § 818(f).

83/ Pub. L. No. 112-81, § 818(f)(2).

84/ Pub. L. No. 112-81, § 818(f)(1) (referencing Ike Skelton National Defense Authorization Act for Fiscal Year 2011, Pub. L. No. 111-383, § 893(f)(2)).

85/ Pub. L. No. 112-81, § 818(b)(3).

86/ Pub. L. No. 112-81, § 818(b)(4) & (5).

87/ Pub. L. No. 112-81, § 818(c)(2)(A).

88/ Pub. L. No. 112-81, § 818(c)(2)(B).

89/ Pub. L. No. 112-81, § 818(c)(3).

90/ Pub. L. No. 112-81, § 818(c)(3)(A).

91/ See 79 Fed. Reg. 26092, 26095–96, 26097 (May 6, 2014).

92/ Pub. L. No. 112-81, § 818(c)(3)(B).

93/ Pub. L. No. 112-81, § 818(c)(3)(C).

94/ Pub. L. No. 112-81, § 818(e).

95/ Pub. L. No. 112-81, § 818(c)(4).

96/ Pub. L. No. 112-81, § 818(h) (amending 10 U.S.C.A. § 2320).

97/ 10 U.S.C.A. § 2320(a), (b).

98/ 10 U.S.C.A. § 2320(b).

99/ 10 U.S.C.A. § 2320(b).

100/ 79 Fed. Reg. 26092.

101/ 79 Fed. Reg. 26092.

102/ 78 Fed. Reg. 28780 (May 16, 2013)

103/ 79 Fed. Reg. 26092.

104/ See 56 GC ¶ 230.

105/ DFARS 246.870-2, 252.246-7007.

106/ DFARS 246.870-2, 252.246-7001; see Vanek & Tibbets, Feature Comment: Proposed FAR Rule Looks To Expand Reporting Of Nonconforming Items, 56 GC ¶ 215 (July 9, 2014).

107/ DFARS 246.870-3(a).

108/ DFARS 236.870-3(b).

109/ 79 Fed. Reg. 33164 (June 10, 2014); see Vanek & Tibbets, Feature Comment: Proposed FAR Rule Looks To Expand Reporting Of Nonconforming Items, 56 GC ¶ 215 (July 9, 2014).

110/ DFARS 202.101, 252.246-7007(a).

111/ DFARS 202.101, 252.246-7007(a).

112/ DFARS 202.101, 252.246-7007(a).

113/ DFARS 202.101, 252.246-7007(a).

114/ 79 Fed. Reg. at 26093.

115/ 79 Fed. Reg. at 26093.

116/ 79 Fed. Reg. at 26093.

117/ 79 Fed. Reg. at 26093.

118/ DFARS 202.101, 252.246-7007(a).

119/ 79 Fed. Reg. at 26093.

120/ DFARS 202.101, 252.246-7007.

121/ S. Comm. on Armed Services, Inquiry Into Counterfeit Electronic Parts in the Department of Defense Supply Chain, S. Rep. No. 112-167, at 1 (May 21, 2012), available at https://www.congress.gov/112/crpt/srpt167/CRPT-112srpt167.pdf.

122/ DFARS 202.101, 252.246-7007(a).

123/ See FAR subpt. 3.10.

124/ When the FAR Council issued the "mandatory disclosure rule" in 2008, it described the relationship between "credible evidence" and contractors' preliminary investigation steps as follows: "The Government does not direct companies to investigate. In the normal course of business, a company that is concerned about ethical behavior will take reasonable steps to determine the credibility of allegations of misconduct within the firm. It is left to the discretion of the company what these reasonable steps may entail." 73 Fed. Reg. 67064, 67087 (Nov. 12, 2008).

125/ 79 Fed. Reg. at 26095.

126/ 79 Fed. Reg. at 26095.

127/ DFARS 246.870-2(b)(5), 252.246-7007(c)(5).

128/ DFARS 246.870-2(b)(5), 252.246-7007(c)(5).

129/ DFARS 202.101, 252.246-7007(a).

130/ DFARS 202.101, 252.246-7007(a).

131/ Pub. L. No. 112-81, § 818(c)(3)(A)(i).

132/ DFARS 246.870-2(b)(5), 252.246-7007(c)(5).

133/ DFARS 252.246-7007(c)(5).

134/ DFARS 246.870-2(a).

135/ DFARS 252.246-7007(c)(1)–(12).

136/ DFARS 252.246-7007(c).

137/ See DFARS 252.242–7005.

138/ DFARS 252.246-7007(d).

139/ See https://www.dcma.mil.

140/ DFARS 246.870-2(a).

141/ DFARS 252.246-7007(c)(4).

142/ 79 Fed. Reg. at 26097.

143/ DFARS 252.246-7007(c)(4).

144/ 79 Fed. Reg. at 26097.

145/ DFARS 211.274-2.

146/ 79 Fed. Reg. at 26097.

147/ DFARS 252.244-7007(7).

148/ 79 Fed. Reg. at 26098.

149/ DFARS 252.244-7007(6).

150/ Pub. L. No. 112-81, § 818(b)(4) & (5), (c)(4); DFARS 252.244-7007(6).

151/ 79 Fed. Reg. at 26099.

152/ 48 CFR 9903.201-1(b)(6).

153/ 79 Fed. Reg. at 26099.

154/ DFARS 252.246-7007(e).

155/ DFARS 252.246-7007(c)(9).

156/ 79 Fed. Reg. at 26099.

157/ 79 Fed. Reg. at 26099.

158/ DFARS 252.246-7007(c)(9).

159/ 79 Fed. Reg. 33164 (June 10, 2014).

160/ See Vanek & Tibbets, Feature Comment: Proposed FAR Rule Looks To Expand Reporting Of Nonconforming Items, 56 GC ¶ 215 (July 9, 2014).

161/ 79 Fed. Reg. 33164.

162/ 79 Fed. Reg. 33164.

163/ See http://www.regulations.gov/#!docketDetail;D=FAR-2013-0002.

164/ See http://www.regulations.gov/#!docketDetail;D=FAR-2013-0002.

165/ 79 Fed. Reg. 33164.

166/ 79 Fed. Reg. 33164.

167/ 79 Fed. Reg. 33164.

168/ 79 Fed. Reg. at 33167; see also FAR 2.101.

169/ 79 Fed. Reg. at 33167.

170/ 79 Fed. Reg. at 33167.

171/ 79 Fed. Reg. at 33167.

172/ See 79 Fed. Reg. 33164.

173/ 79 Fed. Reg. at 33168.

174/ 79 Fed. Reg. at 33167.

175/ 79 Fed. Reg. at 33167–68.

176/ 79 Fed. Reg. at 33167.

177/ 79 Fed. Reg. at 33167.

178/ 79 Fed. Reg. at 33165.

179/ 79 Fed. Reg. at 33167–68.

180/ 79 Fed. Reg. at 33168.

181/ 79 Fed. Reg. at 33167–68.

182/ 79 Fed. Reg. at 33165.

183/ 79 Fed. Reg. at 33167–68.

184/ 79 Fed. Reg. at 33165, -68.

185/ See Council of Space and Defense Industry Associations Comment on FAR Case 2013-002, available http://www.regulations.gov/#!docketDetail;D=FAR-2013-0002.

186/ 79 Fed. Reg. at 33168.

187/ 79 Fed. Reg. at 33167.

188/ 79 Fed. Reg. at 33167.

189/ 79 Fed. Reg. at 33164.

BRIEFING PAPERS