Prepared by

Task Force on Counterfeit Parts of the Committee on Acquisition Reform and Emerging Issues of the American Bar Association Section of Public Contract Law

A White Paper Regarding Department of Defense Implementation of Section 818 of the National Defense Authorization Act for Fiscal Year 2012

October 5, 2012

The Task Force on Counterfeit Parts of the Committee on Acquisition Reform and Emerging Issues of the American Bar Association Section of Public Contract Law is publishing this document to facilitate public discussion of issues relevant to public contract law. The content of the document has not been approved by the Council of the Section of Public Contract Law, the ABA House of Delegates, or the ABA Board of Governors, and does not represent the position of the Committee, the Section, or the ABA.

American Bar Association Public Contract Law Section

Task Force on Counterfeit Parts

Susan Warshaw Ebner, Asmar, Schor & McKenna, PLLC - Chair

Monica Aquino-Thieman, National Air and Space Administration
Erin Alkire, General Electric Co.
Joye M. Anderson, Defense Contract Management Agency
Patricia Becker, Northrop Grumman Co.
Michael Bishop, General Electric Aviation
Jim Burger, Dow Lohnes
Jeffery M. Chiow, Rogers Joseph O'Donnell
David Drabkin, Northrop Grumman Co.
David Edelstein, Asmar, Schor & McKenna, PLLC
Burton D. Ford, Lockheed Martin Co.
Craig A. Holman, Arnold & Porter
Richard Meene, PricewaterhouseCoopers LLP
Robert S. Metzger, Rogers, Joseph O'Donnell
Frank S. Murray, Foley & Lardner, LLP
Joseph Petrillo, Petrillo & Powell
Sherri L. Schornstein, U.S. Attorney's Office for the District of Columbia*
Mary Ita Snyder, General Electric Co.
David Stoughton, Raytheon Co.
Noel L. Woodward, Defense Logistics Agency
W. Hartman Young, Perkins Coie

*****Ms. Schornstein participated in the Task Force and in the review of the white paper.

ABA PCLS Task Force on Counterfeit Parts

White Paper regarding Department of Defense Implementation of Section 818 of the 2012 National Defense Authorization Act for Fiscal Year 2012

I. Introduction

"***No type of company or organization has been untouched by counterfeit electronic parts. Even the most reliable of parts sources have discovered counterfeit parts within their inventories.***"[1]

Counterfeiting has affected governments, businesses, and consumers throughout the course of history. Today, the International Chamber of Commerce estimates the total global economic value of counterfeiting and piracy is as much as $600 billion per year, with the United States suffering the most significant impact.[2] For the federal contracting community, the infiltration of suspect and counterfeit parts into the supply chain has become a considerable concern.[3]

Concerns regarding counterfeit parts in the United States Government's supply chain led to the enactment of Section 818 of the Fiscal Year ("FY") 2012 National Defense Authorization Act ("NDAA FY '12") requiring the Department of Defense ("DoD") to issue regulations regarding the definition, prevention, detection and reporting of actual or suspected counterfeit parts in the defense procurement supply chain.[4] Section 818 further requires the Department of Homeland Security ("DHS") to create a "risk-based methodology" to enhance targeting of counterfeit electronics parts imported into the United

[1] U.S. DEP'T OF COMMERCE, DEFENSE INDUSTRIAL BASE ASSESSMENT: COUNTERFEIT ELECTRONICS 7 (2010).
[2] *See* International Chamber of Commerce, http://www.iccwbo.org/advocacy-codes-and-rules/bascap/about/ (last visited July 30, 2012).
[3] U.S. GOV'T ACCOUNTABILITY OFFICE REPORT, GAO-10-389, DEFENSE SUPPLIER BASE, DOD SHOULD LEVERAGE ONGOING INITIATIVES IN DEVELOPING ITS PROGRAM TO MITIGATE RISK OF COUNTERFEIT PARTS (2010) ("2010 GAO REPORT: MITIGATE RISK OF COUNTERFEIT PARTS"). While the Department of Defense ("DoD") has not yet adopted a Department-wide definition of "counterfeit parts," DoD endorsed a definition that includes genuine parts that have been recycled but which are offered as new. *See* SAE International, *SAE Aerospace Standard 5553, Counterfeit Parts; Avoidance, Detection, Mitigation and Disposition* (April 2009) (defines counterfeit for the aerospace industry and endorsed by DoD). DoD has issued guidance stating that counterfeit materiel is "an item that is an unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source." Memorandum from the Under Secretary of Defense, Overarching DoD Counterfeit Prevention Guidance (March 16, 2012).
[4] National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112-81, § 818(b)(1), 125 Stat. 1298, 1494 (2011) ("Section 818").

States.[5] And it gives the Secretary of Treasury specific permission to disclose to trademark rightholders certain information on detained suspect counterfeit shipments.[6]

Because "[a]lmost anything is at risk of being counterfeited, including fasteners used on aircraft, electronics used on missile guidance systems, and materials used in body armor and engine mounts,"[7] counterfeit parts in the defense supply chain pose safety and national security risks, and "drive up the cost of defense systems,"[8] Issued in advance of DoD's required regulations implementing Section 818, this white paper provides perspectives from a broad cross-section of the government contracting community on the key considerations associated with implementing the legislation's stated goals of avoiding, detecting, and addressing counterfeit parts in the defense supply chain.

A. Brief History of the Counterfeit Parts Problem

A variety of factors have rendered the defense supply chain susceptible to counterfeit parts. First, many deployed U.S. defense systems utilize components that are military and commercial-grade obsolete parts, *i.e.* parts that are no longer made by (or in the inventory of) the original component manufacturer ("OCM") or its authorized dealers.[9] If the OCM or its integrating Original Equipment Manufacturer ("OEM") ceases production, the continuing need for obsolete parts often forces DoD and its contractors to purchase replacement parts from independent distributors, brokers or other sources; this creates a risk that counterfeit parts may be introduced into the DoD supply chain.[10]

---

[5] Section 818(d).

[6] Section 818(g)(1). Jurisdiction over Lanham Act enforcement was retained by Treasury when the Customs Service and Border Patrol were transferred to DHS to form Customs & Border Protection ("CBP").

[7] 2010 GAO REPORT: MITIGATE RISK OF COUNTERFEIT PARTS.

[8] S. COMM. ON ARMED SERVS., INQUIRY INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN, S. REP. NO. 112-167, at iv (2012) ("SASC REPORT: COUNTERFEIT ELECTRONIC PARTS").

[9] *The Committee's Investigation into Counterfeit Electronic Parts in the Department of Defense Supply Chain: Hearing Before S. Comm. on Armed Servs.*, 112th Cong. (2011) ("SASC Hearing: Counterfeit Electronic Parts") (Statement of Sen. Carl Levin)(noting that "The defense community is critically reliant on a technology that obsoletes itself every 18 months, is made in unsecure locations and over which we have absolutely no market share influence").

[10] The United States Senate Armed Services Committee's ("SASC") investigation concluded that "unvetted independent distributors are the source of the overwhelming majority of suspect parts in the defense supply chain." SASC REPORT: COUNTERFEIT ELECTRONIC PARTS at v. Indeed, as a result of the two-year SASC investigation, the SASC's Report announced eight key conclusions:

> **Conclusion 1:** China is the dominant source country for counterfeit electronics parts that are infiltrating the defense supply chain.
> **Conclusion 2:** The Chinese government has failed to take steps to stop counterfeiting operations that are carried out openly in that country.
> **Conclusion 3:** The Department of Defense lacks knowledge of the scope and impact of counterfeit parts on critical defense systems.

Second, counterfeiters have become quite sophisticated at their illegal trade. Counterfeiters continually refine their tactics and processes in order to avoid detection.[11]

Third, counterfeiting is not considered an illegal enterprise in certain countries. To the contrary, certain governments, notably China, permit open counterfeiting, creating a stable environment from which counterfeiters can operate to "manufacture," distribute and sell counterfeit parts openly in public markets or via the Internet without any disclaimers or disclosures.[12] Indeed, "[t]here are dozens of Internet sites that specialize in the trade of electronic parts, with a large number of China-based distributors posting parts for sale."[13] China is not the only country from which counterfeit parts are finding their way into the defense supply chain. Counterfeits may be made in one country and shipped to other countries to be integrated into, or shipped and used in, other parts, equipment, or systems. In addition to foreign sources, there is a domestic counterfeit distribution chain as well.[14]

B. Enactment of Section 818 of NDAA FY '12

In March 2011, the SASC launched an investigation into counterfeit parts in the defense supply chain. This bipartisan investigation identified 1,800 cases of counterfeit electronics in U.S. weapon systems over a two year period from 2009 to 2010, with the total number of suspect parts exceeding one million.[15]

On November 8, 2011, the SASC held a hearing "to explore the problem of counterfeit electronic parts infiltrating critical defense systems and the risk those parts pose to such systems."[16] Shortly thereafter, on November 17, 2011, a bipartisan amendment to the NDAA FY '12 was introduced to "stop

---

Conclusion 4: The use of counterfeit electronic parts in defense systems can compromise performance and reliability, risk national security, and endanger the safety of military personnel.
Conclusion 5: Permitting contractors to recover costs incurred as a result of their own failure to detect counterfeit electronic parts does not encourage the adoption of aggressive counterfeit avoidance and detection programs.
Conclusion 6: The defense industry's reliance on unvetted independent distributors to supply electronics parts for critical military applications results in unacceptable risks to national security and the safety of U.S. military personnel.
Conclusion 7: Weaknesses in the testing regime for electronic parts create vulnerabilities that are exploited by counterfeits.
Conclusion 8: The defense industry routinely failed to report cases of suspect counterfeit parts, putting the integrity of the defense supply chain at risk.

SASC Report: Counterfeit Electronic Parts at vi thru viii.
[11] *Id.* (quoting Vivek Kamath, Vice President of Supply Chain Operations at Raytheon Company).
[12] SASC REPORT: COUNTERFEIT ELECTRONIC PARTS at vi.
[13] SASC Hearing: Counterfeit Electronic Parts (Statement of Sen. Carl Levin).
[14] SASC Report: COUNTERFEIT ELECTRONIC PARTS at 13-14, 16.
[15] *See* SASC REPORT: COUNTERFEIT ELECTRONIC PARTS at 12.
[16] SASC REPORT: COUNTERFEIT ELECTRONIC PARTS at 66.

the importation of counterfeit electronic parts into the United States, address weaknesses in the defense supply chain and to promote the adoption of aggressive counterfeit avoidance practices by DoD and the defense industry."[17] A revised version of the amendment was passed as Section 818 of the NDAA signed by President Obama on December 31, 2011. Ultimately, Section 818 seeks to avoid, detect and mitigate the effects of counterfeit electronic parts throughout the defense supply chain.

II. Legal Analysis of Section 818

A. An Overview

Section 818 imposes a new regime on defense contractors and DoD for the detection and avoidance of counterfeit electronic parts in the defense supply chain. Contractors are to detect and avoid the use of counterfeit electronic parts in supplies and systems delivered to DoD and are responsible for rework or corrective action required to remedy the inclusion of counterfeit parts. Section 818 also requires that, "whenever possible," DoD contractors and subcontractors at all tiers shall obtain electronic parts from original manufacturer of the parts or components (OMs) or their authorized dealers or from "trusted suppliers" who obtain parts exclusively from OMs or their authorized dealers. These policies and procedures must address: (i) Training of personnel; (ii) Inspection and testing of electronic parts; (iii) Processes to abolish counterfeit parts proliferation; (iv) Mechanisms to enable traceability of parts; (v) Use of trusted suppliers; (vi) Reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts; (vii) Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit; (viii) Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts; and (ix) Flow down of counterfeit avoidance and detection requirements to subcontractors. The Section also requires DoD to establish a mandatory reporting program. The law seeks to "eliminate" counterfeit electronic parts from the defense supply chain. DoD also must implement processes, similar to those recently implemented for contractor business systems, for the review and approval of contractor counterfeit compliance systems.[18]

Section 818 takes a holistic approach to the complex problem of counterfeit electronic parts. Parts of the law focus on potential suppliers of components, and aim to improve detection of counterfeits at the borders, enhance the ability to exclude bogus parts from entry into the United States, and toughen enforcement of anti-counterfeiting laws. Other aspects of the law concern the potential buyers and users

[17] S. 1867, Amendment No. 1092, 112th Cong. (2011).
[18] Section 818(e)(2)(B).

of components, targeting the purchasing practices of DoD, its contractors and lower-tier subcontractors and suppliers. An overarching policy of the law is to restrict sources of supply, whenever possible, to OMs, authorized dealers and trusted suppliers, and to better manage decisions to use alternative sources by purchasers of electronic parts and items containing electronic parts, including OMs, suppliers, and ultimately DoD and its contractors and subcontractors.

The law also reaches the use and disposition of electronic parts by contractors by imposing new requirements for receiving inspection, traceability, test and acceptance, and new rules for proper disposition and action on known or suspect counterfeit electronic parts.

There is an information component to the law as well, through the requirement to report counterfeit parts to the appropriate authority and the Government-Industry Data Exchange Program ("GIDEP") or similar DoD-designated program.[19] The law, and the regulations to be issued, will impose obligations for correction, disposition and other remedial action.

The Government, its contractors, subcontractors and suppliers also must address the financial impacts of the new law resulting from the implementation of new processes and procedures, potential increased costs due to limiting suppliers to OEMs, OCMs, and trusted suppliers, and replacement and remedial activity costs. With regard to this latter point, "the 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 [DoD] contracts."[20]

Section 818 implementation will impose additional requirements on contractor systems, and may impact many parts of a contractor's performing organization, including Supply Chain Assurance, Quality Assurance, Purchasing, Engineering, Manufacturing, Product Support, Business Management, Contracts and Finance.

B. Supply-Side Measures

Section 818 seeks to improve the ability of federal officials to detect counterfeit and suspect electronic parts, by strengthening the inspection regime for imported electronic parts. DHS and DoD will establish and implement a "risk-based methodology" for enhanced targeting of electronic parts imported from any country. Further, Congress reaffirmed CBP authority to share unredacted information from and samples of suspect products, their packaging and labels, with the company whose product is suspected of being counterfeited, by specifically authorizing such sharing in order to better identify and exclude

[19] Section 818(c)(4).
[20] Section 818(c)(2)(B).

counterfeit parts at our borders.[21] While clarified CBP authority to resume working with rightsholders, and increased enforcement sanctions, should improve the ability of United States officials to exclude counterfeit electronic parts purchased from foreign sources for import into the United States, there is more to be done. *See* Part IV.B.4.b . Customs, *infra*. While cutting off the supply of counterfeit parts from international sources is an obvious and compelling strategy to deal with the threat posed by counterfeit electronic parts, it does not address the threat from domestic sources of counterfeits.

Successful detection is key to avoidance. Though various laws dealing with counterfeit parts and unauthorized use of trademarks or intellectual property already are in effect, Section 818 amended 18 U.S.C. § 2320 to add a criminal offense for trafficking in military goods or service known to be counterfeit where use, malfunction or failure is likely to cause serious injury or death, impairment of combat operations or other significant harm to national security. The law broadens the definition of the existing "trafficking" offense to include "attempts" or "conspiracy" to traffic in counterfeit military goods or service. Further, definitions of a "counterfeit military good or service" are added to define such item or service as one that is falsely identified or labeled as meeting a military specification, or intended for use in a military or national security application.

The combination of these measures – improved detection, better exclusion at the border, and tougher enforcement –has the potential to cut the inflow of counterfeit electronic parts to U.S. contractors to a significant extent and reduce the risk that parts will be included in delivered defense systems.

C. Demand-Side Measures

As discussed above, contractor purchasing practices are a key focus of Section 818, and changes here seek to reduce the risk of counterfeits, requiring contractors to obtain needed parts from original and reliable sources. The new law requires DoD suppliers, "where possible," to purchase electronic parts from OMs, authorized dealers, or "trusted suppliers." Procedures are to be established to notify DoD of purchases from other than OMs, their authorized dealers and trusted suppliers. Notification will trigger inspection, testing and authentication requirements. DoD must establish qualification requirements under which it will "qualify" trusted suppliers, *i.e.*, requirements to demonstrate that the trusted supplier has appropriate policies and procedures in place. Contractors and subcontractors also will be able to identify and use additional trusted suppliers that comply with "established industry standards" and the pending regulations. When such suppliers are used, however, the contractor/subcontractor is responsible for the

[21] Section 818(g)(1).

authenticity of the suppliers' parts.[22] The selection of such suppliers will be subject to DoD review and audit.

Not all requirements can be met from OCMs, OEMs and authorized dealers, so the new rules on purchasing practices will permit qualification of some independent distributors and brokers. DoD's qualification requirements may include that the would-be trusted suppliers demonstrate designated quality control, maintain documentation of source history and parts pedigree, and possess and provide appropriate certifications.

D. Use & Disposition Measures

As to its own purchasing activities, DoD is to issue guidance and regulations addressing inspection and test of parts (and reporting and quarantining of parts found to be counterfeit or suspect). The details of DoD's implementation of these requirements are yet not available, but contractor obligations are rigorous. Where necessary parts are unavailable from OEMs or authorized dealers, "inspection, testing and authentication" is required when another source is used. Also required are "methodologies to identify suspect counterfeit parts" and systems to detect and avoid counterfeit and suspect electronic parts. A compliant program to detect and avoid counterfeit electronic parts must flow down to subcontractors "counterfeit avoidance and detection requirements." There is no stated restriction on how far down the requirement is to flow.

These additional inspection and test requirements will create new costs. DoD will bear some new costs to the extent contractors allocate such costs to overhead under cost-type and flexibly-priced contracts and when they affect forward-pricing rates for fixed-price contracts.

A compliant contractor program, to detect and avoid counterfeit electronic parts must include "processes to abolish counterfeit parts proliferation." Thus, rather than return suspect parts to the vendor where there is risk of further disposition of dubious parts by resale, the implementing regulations may require that following reporting of such suspect parts, ultimately questionable or counterfeit parts be destroyed unless retained for investigative or evidentiary purposes. This approach would be consistent with Section 818's requirement that contractors have policies and processes to quarantine and dispose of counterfeit and suspect counterfeit electronic parts.

E. Information Measures

[22] Under Section 818, as written, it seems that a contractor is always responsible for the authenticity of parts supplied to DoD no matter the source or circumstance.

Section 818 may increase the availability and retention of information relevant to the detection and avoidance of counterfeit electronic parts in the DoD supply chain, and may improve reporting of such parts to prospective customers, end users and enforcement agencies. For example, Section 818(e) requires covered contractors to have policies and procedures that ensure the traceability of parts. Covered contractors must also flowdown appropriate requirements to their subcontractors.

A contractor or subcontractor that becomes aware, or "has reasons to suspect," that any end item, component, part, or material purchased by DoD contains counterfeit (or suspect) electronic parts, must submit a report on the DoD-designated system within 60 days. And, DoD is to issue new regulations that require reporting "to appropriate Government authorities," under the same circumstances. This may mean that companies at any tier will be required to notify program officers or contracting officers of suspected or actual counterfeit parts. Notably, the rule also requires DoD personnel to submit a report when they become aware or have reason to suspect counterfeits. Section 818 provides that a reporting contractor shall not be subject to civil liability for satisfying its reporting obligations where a "reasonable effort" was made to determine whether a counterfeit or suspect counterfeit part was present. This safe harbor may incentivize cooperation from all tiers of contractors. As noted in Section IV.B.4.d.2 Safe Harbor, *infra*, Section 818(c)(5) regulations should address the logistics and requirements that trigger the safe harbor and other risk issues, such as restrictions on the reporting of foreign events, protection of intellectual property, privacy, and reporting when national security restrictions apply.

The regulations must consider these potentially competing interests to ensure that contractors and their subcontractors can comply with Section 818 reporting requirements without violating other laws, rules and regulations. In addition to regulations, contractors and subcontractors may need to address these kinds of requirements in their contracts to ensure that they get timely and complete information needed for reporting.

F. Financial Measures

The new law treats as "unallowable" the costs of counterfeit and suspect counterfeit electronic parts and of required rework or corrective action. The implementing regulations will need to define what constitutes a "suspect" counterfeit covered by the unallowable cost proscription. Contractors likely will object if DoD treats as unallowable reasonable costs including: costs incurred by contractors to implement the mandated compliance program and processes, costs incurred at the direction of the Government, and costs incurred by contractors to detect or avoid use of counterfeit parts where a part ultimately is not proved to be counterfeit. Contractors may urge that such costs should be treated as

allowable and allocable costs incurred in association with the implementation of the contractor's valid compliance program.

The regulations implementing Section 818 may result in higher direct costs for material, as the law discourages purchasing of parts from "least cost, technically acceptable" sources, in preference to likely more expensive, trusted sources. For example, higher tier purchasers will likely seek to impose more liability on downstream suppliers, and those suppliers may increase price to reflect the additional risks for accepting such liability. There will sometimes be added engineering and manufacturing costs. There will be recurring costs for additional inspection and test, as well as for costs of quarantine and ultimate disposition, and higher overhead costs for many functions whose jobs may be rendered more complex and costly in order to comply with the new requirements.

Financial consequences of the new law may go well beyond costs that can be managed by government contractors. It has been suggested by some contractors that certain sources of supply of electronic parts, including OCMs as well as those that use and distribute such parts (OEMs, dealers/distributors, brokers, etc.), will find it no longer attractive, or economically feasible, to participate in the defense electronics supply chain. Prohibitive costs could arise if DoD and its contractors find they no longer have access to commercial technology and supply sources.

Given that Section 818 requires system audits like the contractor business systems rule[23], DoD may seek to decrement progress payments where a contractor fails to measure up to the requirements of a compliant supply chain assurance system.[24] Such a policy would pose an additional cost risk for contractors.

G. Remedial Measures

Section 818 requires DoD, in its new guidance, to address "remedial actions," including but not limited to suspension and debarment, that will be taken in the case of a supplier that repeatedly fails to detect or avoid counterfeit parts or fails to exercise due diligence. These risks are addressed in more detail below.

[23] Section 818(e)(2)(B) ("establish processes for the review and approval of contractor systems for the detection and avoidance of counterfeit electronic parts and suspect counterfeit electronic parts, which processes shall be comparable to the processes established for contractor business systems under section 893 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383; 124 Stat. 4311; 10 U.S.C. 2302 note).").

[24] *See, e.g.*, Section 818(e)(4).

III. Concern with Potential Non-Use of Rulemaking Procedures

Section 818 required that DoD implement regulations by September 26, 2012. Although Federal Acquisition Regulation ("FAR") and Defense Federal Acquisition Regulation Supplement ("DFARS") cases have been opened, to date no implementing regulations have been publicly issued for notice and comment. The Task Force is concerned that DoD might issue interim rules to regulate activities on the complex and far-reaching issues surrounding counterfeit parts in the supply chain, without transparency and without vetting through a public assessment and comment period. Under the Federal procurement rulemaking provisions, unless there are urgent and compelling circumstances justifying application of an exception or waiver, there will be advance notice of rulemaking before the issuance of agency procurement policy, regulation, procedure, or form.[25] The Task Force believes that, with rare exception, for procurement rulemaking that will impact both government and contractor communities, imposing additional burdens, costs and risks in a complex area such as the handling of detection and avoidance of counterfeit parts in the defense supply chain, the better practice is for agencies to provide the public with an opportunity to assess and comment on the proposed regulations before implementing them. The input from those who will be most affected by requirements imposed by the implementing regulations and who are on the front lines in addressing the counterfeit parts issue and carrying out the regulations on a daily basis is vital to ensuring the viability and ultimate success of the proposed implementing regulations. The Task Force urges DoD to delay implementation of the regulations in interim or final version until it has provided the public an opportunity to review any proposed regulations and submit comments, and until DoD has an opportunity to fully consider and address such comments. Further, since the DoD Guidance issued in March broadly defines counterfeit materiel beyond that of electronic parts, the subject covered by Section 818, the Task Force believes that the regulation of other than electronic counterfeit parts should be done through the normal procurement rulemaking process mandated by Section 1707 of Title 41 of the United States Code so that the public can be provided appropriate notice and opportunity to assess and comment.

IV. Legal Analysis of Section 818

A. Regulating Compliance Requires Definition of the Problem

1. What are "Counterfeit Electronic Parts" and "Suspect Counterfeit Electronic Parts"?

[25] 41 U.S.C. §1707(a)(1), (2) and (d).

In Section 818, Congress has charged DoD with defining "counterfeit electronic part" and "suspect counterfeit electronic part" as part of its implementation of guidance and regulations. Development of clear definition of these and other key terms is critically important because these terms will establish the target and scope of compliance requirements to satisfy Section 818 obligations.

At present, there is no clear, uniform legal definition of what is considered a "counterfeit part" or a "suspect counterfeit part" for purposes of implementation of Section 818. The term varies depending upon the party or parties involved. For example, the Government Accountability Office defined the term "counterfeit parts" as "the misrepresentation of a part's identity or pedigree."[26] In the simplest sense, a counterfeit part may be a part that is fabricated by an unauthorized source or altered by an unauthorized source to pass as a new, genuine part or a part that is represented to be something else. However, more complex questions regarding the definition of a counterfeit must be addressed as well. For example, does the definition of suspect or counterfeit part include:

- Authorized source parts that are diverted from scrap after being rejected?
- A part that is sold by an otherwise authorized dealer, but in a market channel where the dealer lacks authority (so-called "gray market" sales)?
- A genuine part that has been stolen?
- A part used for other than authorized applications?

Under Section 818, DoD was to issue guidance regarding these matters by the end of June 2012.[27] DoD has responded to that obligation, at least in part, through guidance issued in March 2012 ("DoD Guidance").[28] That DoD Guidance defines "counterfeit materiel" as "an item that is an unauthorized copy or substitute that has been identified, marked, and/or altered by a source other than the item's legally authorized source and has been misrepresented to be an authorized item of the legally authorized source." The definition of "counterfeit materiel" in the DoD Guidance does not clearly meet the Section 818 requirements of defining "counterfeit electronic part" or "*suspect* counterfeit electronic part." And, the definition of "counterfeit materiel" that DoD has issued is quite broad; going beyond the scope of Section 818 which is intended to address only suspect and counterfeit *electronic* parts. In addition, there are no definitions of the elemental terms comprising what is "counterfeit materiel," such as "part," "suspect," "actual," and"counterfeit." The definition further should state whether any or all of these elements need to be fulfilled for an item to be considered "counterfeit materiel" or the statutorily-covered "counterfeit electronic part." Further, a used item misrepresented as new is not expressly encompassed within the

[26] 2010 GAO REPORT: MITIGATE RISK OF COUNTERFEIT PARTS.
[27] Section 818(b).
[28] Memorandum from the Undersecretary of Defense for Acquisition, Technology and Logistics to the Secretaries of the Military Departments and Directors of the Defense Agencies, "Overarching DoD Counterfeit Prevention Guidance," March 16, 2012.

DoD Guidance definition of "counterfeit materiel," though Section 818 appears to require this. The DoD Guidance, however, does make clear that such a misrepresentation could subject the contractor to existing procedures (and consequent penalties) for "fraudulent representation."

The DoD Guidance does not address all of the potential scenarios that may involve counterfeit or suspect counterfeit parts, including those that may be most problematic. These electronic components often change hands a number of times before ever reaching the Government customer.[29]

Further, it is unclear whether gray market items, which encompass a significant risk area, are even included in DoD's current definition of counterfeit materiel. A gray market item, for example, may be authentic, but offered for sale by an unauthorized entity that has not properly maintained, stored and inspected the item raising safety, security and product integrity issues.

Another issue to consider is the complexity associated with identifying such parts because it may not always be possible for a contractor to ascertain, at the component level, whether an electronic part in a lower level assembly is new or genuine.

Finally, another issue to consider is whether the definition of "counterfeit electronic part" and "suspect counterfeit electronic part" should be limited to areas such as mission critical applications and/or those impacting potential safety. This option may help limit increased costs by the contractor, and ultimately, the Government as the end-user of a particular electronic component, while simultaneously protecting the most critical components of the defense supply chain.

2. Who Are "Covered Contractors" And What Entities Are Required To Comply With Section 818 Requirements?

Section 818 specifically states that certain portions of the new regulations apply to "covered contractors." The term "covered contractor" is defined as those contractors subject to the Cost Accounting Standards ("CAS").[30] It is unclear whether acceptance of only one contract subject to CAS would render a contractor the kind of CAS-covered contractor that will be subject to these requirements.

Applicability of these requirements to CAS-covered contractors likely will cover all major defense contractors and will require these entities to flow down counterfeit avoidance and detection requirements to their subcontractors. Contractors that are not subject to CAS, such as commercial item

[29] *See, e.g.* SASC Report: Counterfeit Electronic Parts at 14.

[30] Section 818(f)(1) gives the term ''covered contractor'' the same meaning given that term in section 893(f)(2) of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011. Under the Ike Skelton NDAA, 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). This definition does not distinguish between contractors who are subject to full or partial CAS coverage.

contractors or small businesses, apparently would not fall within this "CAS-covered contractor" group. Yet problems with counterfeits do arise in the purchase of commercial items and from sales from other than the OCM or its authorized dealers. Therefore, DoD might opt for broader coverage by applying its rules to contractors who are not subject to CAS.[31] It should be noted that the Senate recognized that the applicability of these requirements to a broader spectrum of contractors and subcontractors would present a set of complex issues requiring close coordination between DoD and the contractor community prior to issuance of any implementing regulations.[32] Thus, if DoD is considering this, The Task Force believes it will be important for DoD to work with and draw comments from industry regarding any such potential implementation.

B. Significant Section 818 Implementation Issues

This paper analyzes the requirements of Section 818 in light of the various segments of the supply chain to identify significant implementation concerns and issues for consideration by DoD and its supply chain community. Given the obvious economic incentives associated with counterfeiting high value parts, certain aspects of the defense supply chain are particularly vulnerable to this problem. Defense electronics often need to operate reliably in adverse, even extreme, environmental conditions. The more demanding performance requirements or environmental conditions to which military parts are subject, the more likely military-grade parts are to justify a price premium over a comparable commercial-grade part, providing economic incentives for counterfeiters. Counterfeiting risk also increases when a part becomes "obsolete." At least four factors make the defense supply chain particularly susceptible to reliance on "obsolete" parts: (1) the relative rigidity of design specifications stemming from the rigorous testing/qualification requirements for military parts/systems; (2) the extended life cycles of major defense systems; (3) the rapid pace of technology turnover; and (4) the Government's diminished market influence over the component supply chain.

Within the supply chain are three broad categories of activities that the Task Force believes a counterfeit compliance program should address: (1) manufacturing, (2) material acquisition, and (3) inspection and quality assurance. Within each of these categories, the program should address the different concerns that arise with regard to the specific requirements associated with detection; exclusion; enforcement; purchasing practices; inspection and testing; reporting; corrective measures; and

[31] For example the DoD Guidance requires program managers to establish testing and verification requirements that will apply to prime contracts, and to subcontracts or suppliers below the prime contracts. The DoD Guidance is not restricted to contracts and subcontracts subject to CAS.

[32] Senate Report 112-173 encourages DoD to solicit input from experts and interested parties to address implementation issues, including which requirements should apply to a broader spectrum of contractors.

improvement of contractor systems. Because there may be special needs for implementation and compliance in different industry areas, the Task Force believes DoD should work with experts in industry to examine the special needs of key defense industry areas and the best ways to address such needs before drafting and implementing specific regulations. Insights regarding some of the kinds of unique issues that might be associated with, for example, Manufacturing, Commercial Items, Supplies, Services, Aerospace, and Energy, are provided below.

1. Trusted Supplier and Authorized Reseller Requirement

As discussed above, whenever possible, Government and covered government contractors should purchase electronic parts in production or currently in stock from the OMs, their authorized dealers or trusted suppliers. Where these parts are purchased from other sources, the law requires that DoD be notified of this fact and that the covered contractor perform inspection, testing, and authentication of the parts that it or its subcontractor obtains. Section 818 also provides that DoD and its contractors and subcontractors may each identify trusted suppliers that may be selling parts to be used in the DoD supply chain. Contractors and subcontractors that identify trusted suppliers must confirm that such suppliers comply with industry standards, and the contractor/subcontractor must assume responsibility for the authenticity of any part provided by a supplier it has identified as a "trusted supplier."

Section 818 directs DoD to include in its regulations "mechanisms to enable traceability of parts" and methodologies to determine whether suspected parts are counterfeit or genuine. Before defining such mechanisms and methodologies, DoD should consult with industry and carefully examine the costs and benefits of the various types of systems. In the event, DoD is considering implementing requirements that effectively might require the replacement of multi-vendor trade secret authentication systems with a common or limited number of systems and methodologies, this kind of consultation is imperative. Imposition of a single or limited number of authentication systems might have the unintended consequence of creating a single point (or limited number of points) of vulnerability that would be vulnerable to target and attack. Section 818 provides DoD with flexibility to employ various approaches through: (1) reviews of contractor systems to detect and avoid counterfeits, and (2) use of a "risk-based" approach to minimize the impact of counterfeits on DoD. Given the size and complexity of the issue, and the evolving nature of counterfeiting, DoD may need to employ multiple and diverse approaches, and to modify the program as it proceeds. The Task Force believes that input from industry, which is

confronting this problem daily would be invaluable in helping DoD and the contractor community to determine which steps might be most effective and efficient.[33]

Under Section 818, DoD is to develop procedures to approve a "trusted supplier," but it must use procedures consistent with 10 U.S.C. § 2319. It is unclear whether this requires DoD to follow all the steps in Section 2319 and implementing regulations before restricting purchases of an item to qualified offerors. In contrast, Section 818 provides that a prime contractor or subcontractor can approve a "trusted supplier" based on "established industry standards," with certain restrictions. This apparent difference should be explored, as it would multiply compliance costs and might complicate implementation if DoD and contractors were to have different approaches for qualifying potential trusted suppliers.

It is important for DoD to best define what would constitute a "trusted supplier" as well as clearly identify the standards and kinds of processes needed for it and its contractors and subcontractors to qualify suppliers as trusted suppliers at every level in the supply chain. If these requirements are too onerous, needed suppliers might refuse to participate, making certain parts potentially inaccessible to DoD. If trusted suppliers will be expected to assume full responsibility for the costs of parts they supply and the unknowable costs of any rework or corrective action, there will be few companies, and likely no responsible small businesses willing to accept liability that exceeds so substantially the costs of the parts they are supplying. In engaging in the development of this guidance, DoD should undertake a risk-based assessment with input from Industry, identifying where the critical issues arise and what is needed to address them effectively and efficiently. This type of close engagement with Industry would assist DoD in developing flexible standards to account for these risks and the various types of contractors and suppliers, which comprise the supply chain, can apply them in a reasonable fashion.

On a broader level, there also should be consistency in developing criteria for a trusted supplier list among federal agencies, particularly those that tend to use the same government contractor community in a particular industry such as aerospace. For instance, Section 1206 of the NASA Authorization Act of 2010, which predates the enactment of Section 818 of the NDAA FY '12 NDAA, requires NASA to establish a "trusted or approved manufacturers" list for electronic parts and specifically identifies potential criteria that may be included.[34] DoD also should consider whether similar criteria are

[33] Strategies used by counterfeiters include, but are not limited to, the "mix[ing of] counterfeit parts with authentic parts, in a method called 'sprinkling' to increase the chance that the counterfeits will avoid detection." See SASC Hearing: Counterfeit Electronic Parts (Statement of Sen. Carl Levin).

[34] *See* NASA Authorization Act of 2012, Pub. L. No. 111-267 §1206(c)(2), 124 Stat. 2805, 2843-44 (2010) ("The criteria may include — (A) authentication or encryption codes; (B) embedded security markings in parts; (C) unique, harder to copy labels and markings; (D) identifying distinct lot and serial codes on external packaging; (E) radio frequency identification embedded into high value parts; (F) physical destruction of all defective, damaged, and sub-standard parts that are by-products of the manufacturing process; (G) testing certifications; (H) maintenance of procedures for handling any counterfeit parts that slip through; (I) maintenance of secure facilities to prevent

feasible. Otherwise, government contractors may find that, depending on the agency, different standards apply for supplying the same electronic component. To that end, DoD may want to contemplate the viability of using FAR Subpart 9.2 to establish a "Qualified Manufacturers List" (QML) or developing other standards under the FAR to ensure consistency throughout the Federal Government for electronic components used in similar industries.

On the issues of trusted supplier and authorized reseller requirements, the Task Force believes that it is important for DoD to consult with Industry regarding any requirements to address these issues.

2. Notification of Source

Section 818 calls for "contractors and subcontractors at all tiers" to "notify" DoD where the contractor sources electronic parts from other than the OCM or OEM, their authorized dealers or trusted suppliers. DoD should consider several issues in determining what regulations are appropriate to implement this requirement such as:

- What level of information will DoD require for this notification?
- Will contractors or subcontractors who do not know the source of a part be required to report as if they were not providing the part from an OEM, OCM, or trusted supplier?
- Will reporting obligations be imposed on a contractor or subcontractor who is not an OEM, OCM, or trusted supplier, but who engages in integration or other manufacture using the part? If so, will it be required to provide specific information regarding its sources of supply and the part(s) themselves, or just the fact that the part comes from an unknown or other than OEM, OCM, trusted supplier source?

Requirements that are too onerous likely will prompt commercial and other suppliers to re-evaluate their continued participation in the government supply chain. Loss of these suppliers and contractors could negatively impact the defense industrial base, drive up costs of obtaining the supplies, and potentially render it difficult or impossible to obtain needed supplies on a timely basis.

It is unclear whether the DoD Guidance requires contractors to provide an explicit representation that an item is "an authorized item of [a] legally authorized source." Such a requirement would add to solicitations a new form of representation containing that phraseology as the current FAR and DFARS provisions do not include such a representations.[35]

Additionally, DoD should ensure it has adequate protections in place to protect proprietary and potentially trade secret contractor or subcontractor information provided in response to any DoD

---

unauthorized access to proprietary information; and (J) maintenance of product return, buy back, and inventory control practices that limit counterfeiting.").

[35] FAR 52.211-5 requires that an offer proposing to supply "used, reconditioned, or remanufactured" provide a "detailed description" of the supplies and obtain the Contracting Officer's approval and imposes similar requirements for offers of unused former Government surplus property. DFARS 252.246-7003 similarly requires post-award notification of potential nonconformities and deficiencies.

notification requirements. Failure to ensure adequate protection of this information may well expose DoD, the contractor and subcontractor to competitive or other economic harms. DoD also should consider including a safe harbor provision in its regulations to protect government contractors and subcontractors against damages arising from problems with parts where reasonable and adequate steps have been taken to vet the parts with reasonable assurance of their authenticity.

3. Establishment of Industry Standards

As noted previously and in the industry-specific sections below, some industry standards presently exist or are in the process of being drafted to address counterfeit parts matters. However, these standards are not all encompassing and may not apply to or translate well across all industries. Some industries do not yet have specific applicable standards in place to address their counterfeit part issues. It is important that the Government take appropriate steps to ensure that DoD guidance and regulations defining the steps necessary to qualify a supplier as a "Trusted Supplier" do not conflict with the terms, definitions, test activities and other components of existing or emerging industry standards.

4. Inspection as a Means to Avoid, Detect, and Deter

Inspection and quality assurance are key components of a system to avoid, detect and deter counterfeit parts problems. The supply chain's inspection and quality assurance links include four essential elements: avoidance, detection, deterrence, and remedies. Each of these points will be addressed in turn.

a) Avoidance

Section 818(b)(2) requires DoD to "implement a risk-based approach to minimize the impact of counterfeit electronic parts or suspect counterfeit electronic parts on the Department, which guidance shall address . . . making sourcing decisions." In making acquisition decisions, DoD and its contractors should have systems in place that review item, price, and supplier risks for procurements. The more data and analytical tools about these three areas that procurement specialists are given to evaluate before a procurement decision is made, the more likely that the contractor's risk of acquiring counterfeit items can be reduced.

Item Risk. Item risk may be evaluated based on item value, criticality, volume, surplus, or ease with which an item can be duplicated or manufactured. For example, controls exist for acquisition of certain types of Critical Safety Items (CSI), which require traceability documentation from non-manufacturers and explicitly states the standards for acceptable trace documentation. Product

Verification Testing (PVT) also may be required based on item risk or supplier risk, or a combination of the two.

Price Risk. In certain circumstances, a bid for an OEM item that is significantly lower or higher than the other bids is an indicator that the item that is being offered is a counterfeit. However, if all of the offers are in the same price range, it is more difficult to detect possible counterfeit items based on offered price. Some analytical tools and algorithms have recently been developed that will be able to better analyze historical pricing and perhaps better indicate whether offered prices are appropriate for items.

Supplier Risk. Perhaps the area that has received the greatest attention in the counterfeit parts realm is supplier risk. Particularly with regard to government contracting, supplier risk is the most difficult to address, because, absent an exception, the Government is directed to obtain contracts through full and open competition and in accordance with the FAR. The FAR includes not only technical, price and past performance elements, but also it may include different socio-economic factors, such as small business set-aside requirements, subcontracting plans and goals. It is difficult to balance the need to protect Government interests in obtaining only genuine microelectronic parts for insertion in military equipment with the need to provide fair and equitable contracting programs that achieve socio-economic goals as well. The regulations should address and balance these various and potentially competing concerns.

One aspect DoD might consider is further use of its supplier registration process. All DoD suppliers must go through a supplier registration process, which involves several different programs and associated systems. They include: (1) the Data Universal Numbering System (DUNS) administrated by Dunn & Bradstreet (D&G); (2) the Central Contractor Registry (CCR) administered by the General Services Administration (GSA); (3) the Commercial and Government Entity (CAGE) program administered by the Defense Logistics Agency Logistics Information Service; and (4) the On-Line Representations and Certifications Application (ORCA) administered by the GSA.
The Federal Awardee Performance and Integrity Information System (FAPIIS) provides specific information on the integrity and performance of covered Federal agency contractors and grantees. Section 818(c)(3) also suggests greater use of trusted suppliers as a method of addressing both item and supplier risk. The objective of a trusted supplier program is to establish and maintain a list of pre-qualified suppliers who have in-place controls that ensure delivery of products that meet specified requirements. Use of Trusted Suppliers ensures quality and reduces product delivery lead times. As noted in the Aerospace and Energy Sections of this White Paper, Sections IV.C.3 and 5, infra, the use of trusted suppliers has been shown to be effective for high-risk items such as fasteners and microelectronics in the past.

b) Detection

Section 818(d) bolsters the inspection requirements for imported electronic parts. Specifically, Section 818(d) requires the Secretary of Homeland Security to "establish and implement a risk-based methodology for the enhanced targeting of counterfeit electronic parts and suspected counterfeit electronic parts *imported from any country*, after consultation with the Secretary of Defense" (emphasis added). In addition, Section 818 aims to enhance the capability of CBP to enforce laws protecting marks by specifically authorizing CBP to disclose certain information to rightholders to assist CBP officers in determining whether suspect merchandise bears counterfeit marks.[36] CBP, under the authority of DHS and the Department of the Treasury, has issued an interim rule,[37] which provides a pre-seizure procedure for disclosing information about imported merchandise suspected of bearing a counterfeit mark for the limited purpose of obtaining the right holder's assistance in determining whether or not the mark is counterfeit. Unfortunately, the interim rule prohibits disclosure until after the importer has seven business days to "satisfy" CBP that the detained shipment is not a counterfeit. Legislation is pending that would require CBP to disclose information upon detention without delay. (H.R. 4216) This new requirement should significantly strengthen CBP's ability to detect counterfeit electronic parts before they enter the U.S. supply chain. DoD should consider CBP's implementation of Section 818 requirements in the development of DoD procurement regulations. Other comments regarding CBP's role and potential actions to address the importation risks are identified at Part IV.B.8, infra.

c) Deterrence

Section 818(b)(3) requires DoD to "issue or revise guidance … on remedial actions to be taken in the case of a supplier who has repeatedly failed to detect and avoid counterfeit electronic parts or otherwise failed to exercise due diligence in the detection and avoidance of such parts, including consideration of whether to suspend or debar a supplier." While the legislation itself may serve as a deterrent, it is not the only deterrent mechanism available to DoD. FAR Subpart 9.4, in practice, already provides agency Suspending and Debarring Officials (SDOs) with the authority to pursue such actions as a cause for debarment under either FAR §§ 9.406-2(b)(1)(i)(B) or (c), or as a cause for suspension under FAR § 9.407-2(c). Specifically, FAR § 9.405-2(b)(1)(i)(B) provides that a debarring official may debar a contractor, based upon a preponderance of the evidence, for violation of the terms of a Government contract or subcontract so serious as to justify debarment, such as a "history of failure to perform, or of unsatisfactory performance of, one or more contracts." Likewise, FAR § 9.406-2(c) (for debarment) and

[36] Section 818(g)(1).
[37] 77 FR 24375-01 (Apr. 24, 2012).

FAR § 9.407-2(c) (for suspension) provide that SDOs with broad authority to debar or suspend for any "cause of so serious or compelling a nature that it affects the present responsibility of the contractor or subcontractor." Repeated failures to prevent and detect counterfeit parts in the government supply chain, particularly those that impact mission or compromise safety, might qualify as a cause so "serious and compelling" that it affects the contractor's present responsibility. DoD should consider this existing suspension/debarment authority in crafting its implementing regulations.

In addition to the "stick" of debarment/suspension, the Task Force believes that a "carrot" of providing positive incentives may aid in the eradication of counterfeit parts from the supply chain. DoD should consider compliance incentives that might be afforded those contractors that have established viable compliance programs that actively take steps to identify and appropriately report and address issues as they arise. Deterrence to malfeasants and appropriate acknowledgement of proper actors are two sides of the coin that should be properly addressed in the implementing DoD regulations.

d) Remedies

Once suspect material is identified, the NDAA includes several requirements regarding the reporting and management of counterfeit goods. Congress likely felt compelled to mandate these practices due to the examples of apparently delayed reporting highlighted in the SASC Report. Nonetheless, many of the new requirements in Section 818 will add costs at multiple levels of the supply chain. For implementation, careful consideration should be given to when these obligations are triggered and the potential ability to streamline the processes mandated for complying with these requirements, including re-evaluation of GIDEP protocols. Below is a discussion of considerations relating to quarantine, reporting, and disposition of suspect counterfeit goods as part of a sound management and reporting program.

(1) Quarantine

Several issues should be considered regarding Section 818's requirement that contractors implement policies and procedures for "quarantining counterfeit parts and suspect counterfeit parts." First, DoD should develop clear criteria to be used by contractors when evaluating whether a part should be deemed "suspect." Counterfeit concerns might arise where the part has unusual markings or appearance, inspection/test failures, paperwork or part traceability gaps, below-market pricing, and sub-tier procurement from high risk sources. It is not clear which of these factors or which combination of these factors might trigger the quarantine and reporting obligations contemplated by the statute. If parts require immediate quarantine, this may impact timely end-item delivery to the war-fighter, and thus, careful consideration should be given in defining when a part will be deemed "suspect." One solution may be to adopt the "credible evidence" standard used under the current FAR Mandatory Reporting Rule.

While this standard is arguably vague, it could provide a threshold standard of proof based on an approach currently used within industry.

Second, DoD should assess protocols for the enforcement of quarantine rules. Although it may be desirable to preserve suspect counterfeit items as evidence for enforcement officials, these protocols should allow contractors to share material with third parties to support their legitimate purposes. For example, contractors should be permitted, during their initial investigation to determine whether there is an actual or suspect counterfeit part, to provide samples to the purported original manufacturer, testing labs, and other government agencies to verify the heritage of the part or identify potential issues. Some of the items may require destructive testing to evaluate material properties. DoD rules might also clarify what, if any, restrictions will be imposed on information that can be shared with the source of any suspect material. The source of the suspect material may possess useful information for evaluating the factual underpinnings of the concern or for determining traceability by identifying sourcing trails and original manufacturer origin. Severe restrictions on communications would likely impair efficient evaluation of true counterfeit risk.

Indeed, there is risk that ongoing civil or criminal or administrative investigations might impair the ability of DoD, its contractors and their suppliers to address these procurement matters with transparency and speed. Procedures and guidance might be identified to aid in addressing these types of situations.

(2) Reporting

The NDAA states that upcoming regulations should require contractors and subcontractors to report suspect counterfeit items "within 60 days to appropriate Government authorities and the Government-Industry Data Exchange Program (or a similar program designated by the Secretary)." The DoD Guidance instructs that counterfeit concerns be reported to GIDEP as well as criminal enforcement authorities. When evaluating the "appropriate" parties that should be included within any reporting obligation, careful consideration should be given to maximizing the likelihood of disclosure to the parties with the most need to know without creating redundant or unduly burdensome reporting structures.

Thus, it is important to consider what information a party is to report, to whom a party is to report, the method by which the report is to be made, and what is to be contained in the report. Below are some considerations associated with various potential reporting channels.

(a) GIDEP

There are some obvious advantages to encouraging or mandating reporting of suspect counterfeit goods into GIDEP. GIDEP has an established communication structure. Many members of the government and contractor community are already GIDEP participating members. The community

already has some practice using GIDEP as a channel for reporting suspect counterfeit goods. Mandatory usage of GIDEP, however, raises some complications. First, not all contractors and subcontractors currently do or can participate. Only U.S. and Canadian companies may participate in GIDEP. DoD should determine how to obtain and provide information about actual or suspect counterfeit parts from contractors and subcontractors who are not able to report through GIDEP. Second, the GIDEP system currently contains export-controlled data which cannot be shared with companies outside the United States or Canada. Use of GIDEP therefore may undermine a legislative aim to abolish counterfeits by depriving contractors and subcontractors who cannot access GIDEP from access to data that would help them to avoid purchasing counterfeit parts from known or unknowable sources. Third, GIDEP currently imposes a number of loosely-defined participation requirements. If contractors are required to become GIDEP participants by virtue of federal regulation, some of these participation requirements – such as the transmission of impact reports – should be re-evaluated in light of their mandatory nature for cost, burden, and reasonableness. Fourth, guidance should be developed that identifies whether DoD or the contractor is the party primarily responsible for transmission of notifications through the GIDEP database to prevent duplicative reporting. Finally, although Section 818 states that contractors shall be immune from civil liability for reporting into GIDEP, the entire procurement community would benefit from clarification as to both the degree of investigation needed to trigger the reporting obligation and the associated immunity. Any regulatory regime that channels reporting through GIDEP will probably warrant a re-assessment of the GIDEP program requirements in general.

(b) Contracting Officer & Government Program Customer

Section 818 also references reporting to the "appropriate" Government authorities. There are strong reasons why both a contracting officer and the cognizant Government program lead should receive those notifications. These individuals are likely to be in a position to assist with coordination and resolution of any product issues (e.g., delivery delays, field replacements), waiver or modification of contractual requirements (e.g., waiver of technical limitation, approval of re-designs), and resolution of contract remedies. Given these practical needs, the Government should identify which Government authority (ACO, PCO, or other administrative contracting official) will be the focal point responsible for official notification to other government constituencies. If this is done, the designated contracting official then could assist with GIDEP reporting to the extent that the contractor faces an impediment to reporting on this vehicle (national security and otherwise), avoiding or eliminating duplicative reporting duties. DoD may also consider identifying one or more enforcement agencies as "appropriate Government authorities" that should receive reports of suspect counterfeit parts. Some may argue that contractors are already obligated to report suspect counterfeit parts to the DoD Inspector General as potential violations

of the False Claims Act ("FCA") that are subject to disclosure under the Mandatory Disclosure Reporting Rule. The elements that trigger liability under the FCA, such as subcontractor awareness of intended DoD usage and the recklessness standard that may apply to management of vendors and subcontractors, however, may raise difficulties. The credible evidence standard used in conjunction with the Mandatory Disclosure Reporting Rule also can be difficult to evaluate. Given these complications, there are reasons why mandatory referral beyond the relevant contracting officer and impacted program should be left to the discretion of the Government rather than automatically imposed on the contractor. Alternatively, to the extent any duty is placed on contractors and subcontractors to report to "appropriate" authorities, it may make sense to align reporting obligations of suspect counterfeit parts with the existing reporting requirements of the Mandatory Disclosure Reporting Rule rather than create new reporting standards and processes.

(c) Safe Harbor

Finally, any regulations should make clear that a safe harbor exists for contractors that provide such reports to the Government. In answer to concerns expressed by industry that a reporting company could be sued, Section 818 provides that a reporting contractor shall not be subject to civil liability for satisfying its reporting obligations where a "reasonable effort" was made to determine whether a counterfeit or suspect counterfeit part was present. Future DoD Guidance should address what constitutes a reasonable effort and other risk issues such as restrictions on reporting of foreign events, protection of intellectual property, or procedures for reporting when national security restrictions apply..

(3) Disposition

Beyond references to quarantine of material, the NDAA does not include concrete requirements relating to disposition of counterfeit material. The DoD Guidance instructs that material should be preserved until resolution of the non-conformance, and if confirmed counterfeit, material should be preserved until an approval for release is obtained from enforcement authorities.

Material disposition raises a number of complications that DoD should examine and address in its regulations. For example: How long should a contractor or government agency reasonably be required to store suspect material? Are some or all of these costs allowable? Could destruction of suspect or confirmed counterfeit material after a reasonable period of time meet Section 818 prevention requirements? If contractors and government agencies are required to preserve material until receiving affirmative disposal instructions from government enforcement authorities, how will potentially conflicting requirements be addressed, *e.g.*, pressure on enforcement officials to allocate attention to pressing cases versus closing out less pressing matters that might be impacting performance of defense contracts? In light of these complications, clarification of disposition requirements might be more

effectively addressed after the benefit of discussion with industry and further actual experience. Contractor and government agencies already have duties to preserve evidence in light of existing civil and criminal standards. The imposition of additional disposition limitations at this point may drive up contractor and end item costs without providing a corresponding level of additional benefit.

(4) Concerns with an Audit and Business Systems Rule Approach

Within the defense electronics supply chain some are concerned that since Section 818 requires system audit comparable to that under the business systems rule, DoD could decrement progress payments if a contractor fails to evidence a compliant supply chain assurance system. Where the threat of counterfeit parts is evolving and requirements are not all in place, care should be taken to establish clear standards for what specific systems and actions are required of a contractor or subcontractor before any contractor business systems rule-type audit and decrement processes are considered for adoption. The Task Force urges DoD to engage in a dialogue with the public to determine what aspects of the contractor business systems rule may be applicable to the counterfeit parts regime and how best to employ them before any rule is drafted and then implemented.

(5) Existing Remedies

Unlike many other industries, aerospace-unique penalties associated with fraudulent parts already exist. Title 18 of the United States Code imposes criminal and civil penalties for fraud involving aircraft or space vehicle parts, including making it a Federal criminal offense to knowingly and with the intent to defraud falsify or conceal a material fact concerning any aircraft or space vehicle part. Specific penalties may be imposed if the offense relates to the aviation quality of a part installed on an aircraft or space vehicle. The new criminal and civil penalties associated with Section 818 are in addition to the pre-existing regime and potentially create another compliance challenge.

Any revised regulatory regime that arises as a result of Section 818 may present numerous legal risks. Some of these, discussed above, are referenced in the legislation itself. Other risks exist because either the United States or private whistleblowers may base a case of fraud on regulatory violations. Some of the fraud cases contractors face – such as FCA cases[38] – are increasingly tied to contractual, statutory, or regulatory violations as a result of an "implied certification" theory. Even where a contract does not specifically state that a contractor must adhere to a particular regulation as a precondition of payment, liability nonetheless may attach where that violation was "material to" the Government's

[38] 31 U.S.C. § 3729 *et seq*. Under the *qui tam* provisions of the FCA, private whistleblowers or "relators" may bring an action in the name of the United States, and may share in as much as 30 percent of the proceeds the government ultimately recovers. 31 U.S.C. §3730(b)-(d).

decision to pay. Depending on the type of regulatory noncompliance alleged, the risks can be substantial. Questions exist regarding whether the current fraud environment relating to regulatory violations amounts to a "strict liability" type regime where any regulatory noncompliance – even a trivial one – could result in FCA liability.

Section 818 requires that DoD's forthcoming regulations address "any rework or corrective action that may be required to remedy the use or inclusion of" counterfeit (or suspect counterfeit) electronic parts. The regulations also should address situations involving the selection of "trusted suppliers" for whom contractors "assume[ ] responsibility" in the event of a noncompliance, and the regulations will implement a 60-day reporting requirement for contractors who become aware of (or have reason to suspect) the inclusion of noncompliant parts. Thus one can imagine situations in which a failure to adhere strictly to the new regulations might result in an argument that such noncompliance was fraudulent because it was "material to" the Government's decision to pay. Depending on when contractors make certain representations concerning counterfeit electronic parts, cases further may arise alleging that the entire contractual undertaking was fraudulent under a "fraud in the inducement" theory.

The existence of the NDAA's limited "safe harbor" highlights the enhanced risk for those that fail to meet the 60-day reporting requirement. Risk is enhanced also for those that fail properly to identify trusted suppliers or properly "assume responsibility" for them and for those that invoice the Government for replacement or rework costs, even if inadvertently.

Any regulatory guidance should take into account these risks. DoD may want to consider other types of safe harbors as well for inadvertent noncompliance especially in spite of reasonable diligence. The issue of trusted suppliers presents unique issues because, even though the regulations encourage the identification and use of trusted suppliers that comply with "established industry standards," it is not clear what standards are to be used and how "established" they are. Assertions that contractors make concerning their "trusted suppliers" need not be yet another area where contractors take on undue or undefined risk. The regulatory guidance should take into account not only the risks that are identified in the legislation itself, but also consider risks that were not.

3. Government as Trusted Supplier

Regulatory guidance should address the Government's various roles, including its role as a supplier of electronic parts. Under numerous contracts and grants, DoD provides third-party parts and equipment as Government Furnished Material (GFM) to other government agencies, grantees, contractors and their subcontractors. Thus DoD also should ensure that it is a trusted supplier of the items it furnishes

as GFM, and should assess what, if any, acquisition and storage requirements or special treatment these supplies are to be afforded while in Government custody.

Government's role as trusted supplier should entail more than just ensuring that it has purchased from appropriate suppliers. It should ensure that while the supplies are in the Government's control, they are being properly maintained and managed to prevent counterfeit risks. Under established contract clauses and case law, contractors are entitled to suitable, sufficient and adequate GFM. When the Government provides inadequate, insufficient or unsuitable GFM, contractors are entitled to compensation through changes or claims. Where contractors receive GFM, DoD should consider a safe harbor from any liability or potential damages arising from the use of such Government-provided parts. If DoD requires contractor or subcontractor action to authenticate GFM, that should be clearly identified and the contractor appropriately compensated for such added duties.

4. Gray Market

Gray market activities may cause significant practical difficulties in developing DoD regulations. DoD should assess whether, and the extent to which, the gray market will be a permissible avenue for purchase of defense supply chain parts, especially those that are out-of-production. Various statutes impose civil and criminal penalties associated with counterfeit parts and unauthorized use of trademarks.[39] The intersection between "gray market" goods and counterfeit parts, however, is less than clear. In certain instances, the two areas overlap, such as when goods are improperly marked with the trademark or other markings of the OEM and sold as something that they are not. In other cases, the Federal Courts have defined "gray market goods" as authentic goods that have been manufactured and legitimately sold outside the United States, but are imported into the United States without the authority of the U.S. trademark-holder.[40] Thus, "gray market" goods may be authentic OM goods that are considered "gray market" simply by virtue of being sold in the United States market by an unauthorized dealer or through unauthorized sales channels.[41]

Section 818(b)(1) directs DoD to *include* "previously used parts represented as new" within the definition of "counterfeit electronic part." The DoD Guidance clarifies that a used item represented as a

[39] *See, e.g.*, 19 U.S.C. § 1526; 19 U.S.C. §1595; 15 U.S.C. §§ 1124-1125; 18 U.S.C. §2320.

[40] *See Omega SA v Costco Wholesale Corp, Omega S.A. v. Costco Wholesale Corp., 541 F.3d 982 (9th Cir. 2008), aff'd by an equally divided court,* 131 S.Ct. 565 (2010); *John Wiley & Sons, Inc. v. Kirtsaeng,* 654 F.3d 210 (2d Cir. 2011).

[41] For example, in certain circumstances, the Defense Supply Centers may sell authentic parts to contractors or buying commands, yet the Center may not be an OEM/OCM authorized distributor or reseller of such parts. While none of these parts are in the strictest sense "counterfeit," they can be problematic. Additionally, as noted above, some obsolete parts may only be available from unauthorized after-market sources.

new item may also be subject to fraudulent representation procedures. Yet it is unclear how authorized parts from unauthorized sources are to be treated in the federal procurement context. Further electronics parts are easily damaged (or no longer work within specification) when not properly handled (*e.g.*, subject to electrostatic discharge, moisture or physical abuse). Unauthorized sources may not have the appropriate training and, accordingly, may handle or store parts contrary to OEM requirements, thereby damaging the parts or increasing the risk that they may not ultimately perform within specification even though manufactured by the OEM.

5. Allowability of Costs

There are inevitable costs associated with the avoidance, discovery and handling of counterfeit parts. Current legislation indicates reluctance on the part of the Government to pay those costs, instead there is a noted intention to force contractors to bear those costs, as much as possible.[42] A robust anti-counterfeiting program probably means increased costs for contractors so it is unrealistic for the Government to expect contractors not to pass those costs on in the form of higher prices.[43]

The new law treats the costs of required rework or corrective action due to counterfeit electronic parts as "unallowable." Other types of costs associated with the requirements of Section 818, and the treatment of such costs are not explicitly addressed. These may include costs of general compliance, *i.e.*, the new systems, policies and procedures that the law requires or makes advisable. There also may be higher direct costs for material, as Section 818 certainly operates to discourage purchasing of parts from "least cost, technically acceptable" sources, in preference for possibly more expensive, trusted suppliers such as OCMs, OEMs and authorized distributors.[44] Such costs, if they are reasonable, should be treated as allowable and allocable costs incurred in association with the implementation of the contractor's valid compliance program.[45] Financial consequences of the new law, if not fairly and appropriately addressed, may go beyond costs that can be managed by individual government contractors. It is possible that some

[42] NDAA § 818(c)(2).

[43] Also of concern is whether the Government can find the resources necessary to perform its own role in detecting and preventing counterfeiting. At a minimum, there may have to be increased Government enforcement actions when counterfeiters are identified. *See* recommendations in Customs Section, IV.B.8, *infra*.

[44] Examples of the additional costs associated with implementation of the new law include (1) increases in supplier prices as contractors seek to impose more liability on downstream suppliers; (2) added engineering and manufacturing costs associated with, for example, design of new parts or assemblies to address a shortage of original-source parts or imposition of certain marking requirements to validate authenticity of parts; (3) recurring costs for additional inspection and test, as well as for costs of quarantine and ultimate disposition, and (4) higher overhead costs for many functions whose jobs will be rendered more complex and costly in order to comply. In addition, many companies will experience significant non-recurring costs for the development and implementation of new policies and procedures, including those to perform risk-based assessments of counterfeit materiel risk.

[45] FAR 31.201-2.

sources of supply of electronic parts, including OCMs as well as those that use and distribute electronic components (OEMs, distributors, brokers, etc.), will find it no longer attractive, or economically feasible, to continue to participate in the defense electronics supply chain.

Last, since Section 818 contains express language regarding the unallowability of costs for rework and corrective action, it will be important to address situations in which rework and corrective actions arise from causes outside of the contractor's care and control, such as when counterfeits are included in GFM or contractor furnished material ("CFM").

6. Traceability and Marking

A significant issue in the counterfeit electronic parts area is continuing program needs for obsolete and unavailable parts. Such parts are likely targets of counterfeiters. It is important to realize, however, that in this area certain prevention mechanisms preferred by Section 818 — dealing with OMs, authorized dealers and trusted suppliers — are least likely to be effective.[46] Systems and procedures to assure the chain of authenticity and traceability of parts are likely to be required in the implementation of Section 818 regulations by DoD. However, because many parts are obsolete and unavailable from OEMs, OCMs, and trusted suppliers, authentication may be complex and costly. There are methods to attempt to reduce the need for obsolete parts, or at least plan for it, but those approaches should be vetted by DoD and Industry together to determine what is appropriate in different circumstances.

Another area of concern involves the requirement for traceability of parts. It is probably not feasible to expect every electronic component in every item of supply to be traceable back to its original source. Manufacturers frequently draw some supplies from stock, particularly for common, low-cost items, and especially for commercial items. It is important to identify which items need to be traced before they are purchased. A risk-based approach to this issue makes the most sense.

For the most critical items, serial numbers or other unique identifiers might be necessary.[47] However, determining which are the most critical items and what are the appropriate marking and identification methods are decisions and activities that need to be planned out well in advance of manufacturing.

---

[46] Indeed, Section 818's emphasis on limiting suppliers might have the effect of reducing the development of alternative sources of supply that might be of greater longevity.

[47] *See* DFARS Case 2009-D018, Warranty Tracking of Serialized Items, 76 Fed. Reg. 33166-01 (June 8, 2011): "Additionally, as counterfeit items, particularly electronics parts increase, this traceability of items to a warranty will assist all members of the supply chain to manage risk appropriately. This traceability also leads to ensuring the Government receives the supplies purchased, reducing the number of counterfeit items. Based upon the above, DoD published a final rule." *Id*.

It should be noted that attempts to apply markings or unique identifiers mid-stream or after-the-fact, once the parts have left the manufacturing facility or are already out of production, may well impose significant costs and higher risks. This kind of after-production effort may prove impossible to implement effectively or efficiently. Where parts are already out of production, for example, one would have to address issues such as how these parts might be marked, who would be authorized to mark them, who would absorb these additional costs, whether the part to be marked is authentic, and whether it is even possible to locate and mark all outstanding authentic parts. Hence, a fact- and risk-based approach to mitigating the counterfeit parts issue cannot be a simple across-the-industry solution on day one, but should be a calculated, phased-in deliberate method.

7. Intellectual Property Implications

Counterfeit parts matters implicate various aspects of intellectual property. Care should be taken to assure that contractor intellectual property is not misused and that the rights of the contractor, its subcontractors and vendors are not compromised. It is important not only because bona fide intellectual property holders need their investments protected for economic reasons, but also because the inadvertent or unauthorized disclosure of intellectual property to aid in the detection, avoidance, and reporting of counterfeit parts may, if disclosed to the wrong parties, result in additional and harder to detect counterfeits.

Materials, parts, components, equipment, systems, processes and information on the supply chain itself all contain intellectual property of one type or another that needs to be appropriately handled and protected. Intellectual property in the form of patented inventions will need to be handled in accordance with appropriate licensing agreements. Other proprietary trade secret intellectual property should be appropriately identified and the applicable rights established. Items that are not themselves subject to protection, because they have been publicly disclosed, have been developed wholly at Government expense, or the patent or other protection period has expired, still must be handled carefully to address any intellectual property issues regarding the disclosure of contractor, subcontractor or vendor supply sourcing data that is proprietary, trade secret or competition sensitive. The need to protect against unauthorized or inadvertent disclosure of protected data should be balanced against the needs of contractors and subcontractors at all tiers to obtain sufficient information about the items they acquire, use and deliver to others to determine whether they are genuine or counterfeit or suspect counterfeit parts. Undoubtedly, major defense contractors will require their subcontractors to authenticate parts. Whether these efforts will suffice remains to be seen. DoD should consider whether its existing intellectual property regime provides adequate assistance to its program to identify counterfeits and exclude them

from the supply chain. This may also be an area where cooperative efforts with industry can provide cost-effective solutions.

Another consideration regarding intellectual property rights and how they impact DoD's ability to mitigate the risk of counterfeit parts would be DoD's ability to obtain the intellectual property rights or technical data necessary to commission production of obsolete parts that are at high risk of being counterfeited. Obtaining those rights will not always be practical or even possible, if the component at issue is a commercial item (developed at private expense) and the original component manufacturer is unwilling to license or sell its rights in a particular out-of-production component to allow DoD to commission new production runs of verifiably authentic parts. Likewise, Section 815 of the NDAA FY '12 may provide DoD an ability to obtain certain technical data necessary for the segregation or reintegration of an item or process if the technical data is needed for the purpose of reprocurement, sustainment, modification, or upgrade of a major system or subsystem thereof, a weapon system or subsystem therefore, or any noncommercial item or process.[48] DoD should be thinking about the entire procurement life cycle, including program planning, procurement, selection and contract negotiation, and contract administration to determine the kind and type of technical data it will need in order to address counterfeit problems at the front end, by assuring a steady means of ongoing production and/or stocking of genuine items, and also throughout the life cycle to assure that it has or can obtain the information needed to enable it to properly avoid and detect actual or suspect counterfeits.[49] Because intellectual property amounts to a contractor's, subcontractor's or vendors "crown jewels," DoD should exercise care in determining what intellectual property it will require and the means by which it will obtain and protect it. DoD should consult with industry on this issue to identify appropriate types of data needed and methods for its acquisition and protection so as to minimize the risks associated with the use and dissemination of intellectual property.

8. Customs

Implementation of Section 818 requirements by DoD should be part of a multilayered approach to prevent counterfeits from entering the government procurement supply chain and into government-acquired products. While Section 818 does not include specific deadlines for implementation of regulations regarding the role the CBP has with regard to the interdiction and control of actual and

[48] Pub. L. No. 112-81, § 815(a).

[49] There are semiconductor companies specializing in contracting with OCMs to stock (and in some cases, license the intellectual property, and obtain wafers and dies to manufacture) semiconductors OCMs no longer will produce. In considering life cycle procurement, DoD might consider working with such OCM-authorized companies to ensure that critical components will be available from such authorized sources for the life of the end product.

suspect counterfeit parts, our white paper would be remiss if it did not address the urgent need for the first layer of defense against counterfeit parts to include activities at the border before the parts can enter the domestic portion of the government procurement supply chain. Congress has charged CBP with seizing counterfeits before they enter the country.[50] In the past, CBP worked with the rightholders of authentic parts (*i.e.*, the manufacturer legally allowed to apply its trademark to the product or, as used above, the authorized source). CBP stopped providing rightholders' unredacted photographs of detained electronics parts and their product labels because of concerns related to the Trade Secrets Act[51] and the protection of the gray market.[52] In the past, these photographs enabled the rightholders to rapidly and efficiently identify counterfeits[53] and permitted CBP to quickly seize counterfeits and release genuine imports.

In addressing the border problem, NDAA Section 818(g) provides, in pertinent part, that where CBP:

> [S]uspects a product of being imported in violation of section 42 of the Lanham Act, and subject to any applicable bonding requirements, the Secretary of the Treasury may share information appearing on, and unredacted samples of, products and their packaging and labels, or photographs of such products, packaging, and labels, with the rightholders of the trademarks suspected of being copied or simulated for purposes of determining whether the products are prohibited from importation pursuant to such section.[54]

Reinstatement of this authority to CPB Officers to share information with rightholders, without conditions, should greatly assist in the avoidance and interdiction of counterfeits.

In addition to steps to be taken by CBP, DoD should coordinate with CBP, OEMs and OCMs to determine how its regulations might best be implemented in concert with the CBP provisions of Section 818. Ensuring a close working relationship with CBP would have an added salutary benefit - putting criminal importers of counterfeits into jail and out of business and deterring others.

C. Industry Specific Concerns

1. Commercial Items

---

[50] The authority Congress delegated to Treasury and CBP under the Tariff Act is to inspect imports (19 U.S.C. § 1499(a)) and detain them if additional time is necessary to confirm that the imported merchandise does, in fact, comply with U.S. law (*Id.* § 1499(c)). The Lanham Act prohibits importation of merchandise bearing a counterfeit, copy or simulation of a registered trademark. 15 U.S.C. §§ 1526(a), 1124, 1125(b).

[51] 18 U.S.C. § 1905.

[52] 47 Fed. Reg. 24375, 24377 (April 24, 2012)

[53] *United States of America v. Stephanie A. McCloskey*, Government's Consolidated Memorandum in Aid Of Sentencing and Motion for Downward Departure Pursuant to U.S.S.G. § 5K1.1 at n.11. ("*McCloskey*") (Available at http://media.cmgdigital.com/shared/news/documents/2011/11/01/mccloskey_sentencing_memo.pdf) and House Hearing at 1-2.

[54] NDAA § 818(g)(1).

Section 818 does not specifically address which of its requirements are applicable to commercial and commercial-off-the-shelf (COTS) item manufacturers and suppliers. For example, under Section 818(c)(2)(A), as noted previously, there is a specific provision regarding the requirement that "covered contractors" are responsible for "detecting and avoiding the use or inclusion of counterfeit electronic parts or suspect counterfeit electronic parts in such products and for any rework or corrective action that may be required to remedy the use or inclusion of such parts." Per the definition of covered contractor in Section 818(e), only CAS-covered contractors are to be subject to these provisions. Since the FAR provides an exemption to CAS for commercial items, it stands to reason that Section 818 should not apply to commercial or COTS contractors. However, Section 818 also provides that "covered contractors" are required to flowdown "counterfeit avoidance and detection" requirements to their subcontractors, and it does not specify whether this will be a required flow down for all or only some tiers. However, Section 818 provides that DoD regulations require:

> **[C]ontractors and subcontractors at all tiers** – (1) obtain electronic parts that are in production or currently available in stock from the original manufacturers of the parts or their authorized dealers, or from trusted suppliers who obtain such parts exclusively from the original manufacturers of the parts or their authorized dealers; and obtain electronic parts that are not in production or currently available in stock from trusted suppliers. [55]

Thus, Section 818's notice requirements if the parts supplied are not from one of these identified suppliers or manufacturers (818(c)(3)(B)); its qualification, identification and use requirements for trusted suppliers (818(c)(3)(C)); and its reporting requirements (818(c)(4)), all apply to both contractors and subcontractors, including apparently those not identified as "covered contractors."

There are specific provisions in other legislation that support restricting coverage of at least some of the provisions of Section 818 to non-commercial items. Specifically, 41 U.S.C. §1907 makes inapplicable to COTS items subsequent laws that do not reference Section 1907, unless the Administrator of the Office of Federal Procurement Policy ("OFPP") makes a determination that it is in the Government's best interests that the new law apply to COTS items.[56] Section 818 does not specifically refer to 41 USC §1907. Further, the Committee Report on the Senate version of the NDAA for FY 13 asks DoD to answer following question: ". . . To what extent should suppliers of commercial, off-the-shelf end items be excluded from coverage pursuant to the authority of Section 1907 of title 41, United States Code? . . ."[57] Thus, application of the requirements of Section 818 to all or only specified groups of government contractors and subcontractors should be clearly identified and addressed in the

[55] NDAA § 818(c)(3)(A) (Emphasis added).
[56] 41 U.S.C. § 1907(b)(2).
[57] National Defense Authorization Act for Fiscal Year 2013 Report to Accompany S. 3254, Report No. 112-173 at 152, Items of Special Interest (June 4, 2012).

regulations. Whether and how to include these groups in coverage under the regulations and guidance is a matter that should be the result of discussion with industry and the public regarding the risks, pros and cons of inclusion. Ultimately, at least for COTS items, the decision to subject COTS items to the requirements of Section 818 is the responsibility of the OFPP.[58] Such a determination should be supported by some analysis of the impact the application of Section 818 to COTS items and be subject to public review, if not comment.

In gathering information for the preparation of this white paper, the authors were provided information indicating that a number of COTS item manufacturers had met with Congressional offices and with DoD, and advised that the application of Section 818 to COTS items would be inconsistent with their current market practices, even though they are opposed to counterfeit items and believe the infiltration of counterfeit items into their supply chain damages their products' reputation, market share and product performance. These COTS item manufacturers noted that it generally is their practice to replace non-conforming products under their commercial warranties and, absent some unusual circumstance, for example statistically significant failure rates, they do not conduct a forensic examination of the failed product. Also, they pointed out that their commercial liability is generally limited to the replacement of the non-conforming/failed product. Section 818 would increase their potential liability beyond their capacity to cover the new virtually unlimited liability provisions of Section 818. These manufacturers of COTS items have observed that applying Section 818 to their products would have several potential impacts:

- Some would cease doing business with the Federal Government altogether, as their sales to the Federal Government represent such a small percentage of their overall sales that it would be cost prohibitive for them to change their practices to implement the requirements of Section 818.
- Other manufacturers have indicated that to comply with the requirements of Section 818 would require them to establish a separate manufacturing line for Federal Government customers, thus increasing the costs to the Federal Government, because the products sold to the Federal Government would need to bear the full overhead cost of the Government-unique production line, sacrificing the efficiencies that would have otherwise been realized by sharing overhead costs of a single common Government-*and*-commercial production line.
- For those companies selling COTS items, that continue to do business with the Federal Government, Section 818 requirements could deny the Government immediate access to the latest commercial technological developments, due to the time lag that would be needed to establish the separate Government-unique production line that would be necessary for some manufacturers to address the new requirements of Section 818.

Given the foregoing potential impacts, it would be advisable that DoD engage in a dialogue with Industry (including commercial item and COTS suppliers) to determine what can be done and the best way to do it without impairing the availability of needed parts for the defense procurement supply chain.

[58] 41 U.S.C. § 1907(a)(2).

2. Services

A significant portion of government contracting today involves the provision of services to the Government. Services purchased by the Federal Government come in many different variants, ranging from fairly low-skill services, such as facilities maintenance and grounds-keeping services, to very specialized, highly trained professional services, such as systems engineering and technical assistance (SETA). Several aspects of the new Section 818 requirements may affect the providers of services to the Federal government and may pose unique challenges to the implementation of that Section's requirements in the services context.

First, services contractors and subcontractors may have unique responsibilities and potential vulnerabilities with regard to Section 818 requirements relating to the prevention, detection and reporting of suspected counterfeit parts. These contractors may purchase parts or equipment for performance of their services. Additionally or alternatively, they may be provided higher level contractor furnished equipment or government furnished equipment that they are asked to further develop, integrate, operate or maintain. Questions regarding services providers' roles and responsibilities with respect to Section 818 requirements should be discussed with Industry before being established by DoD. For example, would services providers or their personnel be at risk of producing "counterfeits," if they did not have a specific certificate or agreement from an OEM or OCM to develop or install each item of CFE/GFE software or electronics on the higher-level platforms?

Second, service contractors and their personnel are in a unique position in which they might uncover counterfeit parts before or as they are being installed or used in parts, components, equipment, systems, or facilities vital to the national defense. Because they may not immediately recognize that they are part of the supply chain covered by the requirements of Section 818, it will be important for DoD to develop properly crafted contract clauses and flow downs that indicate to whom service contractors are to report and what they are to do to identify, report and otherwise handle and dispose of suspected or actual counterfeit parts. Such issues need to be carefully thought out and addressed in the services contract context. If services providers contract directly with the Government, they may be asked to handle matters differently than they normally would as lower-tier subcontractors or consultants.

Third, careful thought should be given to determining whic professional and other services providers are covered by the new Section 818 requirements and how they are to be covered under the new regulations. Many of these providers are commercial services providers who price and perform based on their industry's commercial standards. Asking them to act differently for government services contracts and subcontracts, may require them to price, and use, different personnel who are specially trained to

address the Section 818 requirements. New and different requirements for detection and handling of counterfeit or suspect counterfeit parts may be deemed noncommercial and may require different treatment and pricing. *See* IV.C.1. , *supra.*

Fourth, we assume that new regulations or contract clauses may be issued to implement Section 818 requirements. However, the DoD Guidance indicates that existing regulations may be used to address counterfeit parts. Thus, services providers who might not have been concerned about certain clauses in their contracts previously may not be aware that the existing requirements are being enforced and applied to them. Education about these developments will be vital to minimizing the difficulties in applying these strictures to services providers.

3. Aerospace

Members of the aerospace industry, standard-setting organizations, and Government agencies have been concerned about the potential consequences associated with the introduction of counterfeit semiconductors and other electronic parts into the aviation and aerospace supply chain for a number of years. Given the longevity of aerospace platforms and programs and the ability of these platforms to travel anywhere in the world, it is critical that aircraft, satellites and other aerospace products contain high-reliability electronic components. Failures of airplanes in service or products deployed in orbit can be catastrophic. Removal and replacement of components contained in deployed space vehicles and satellites is often not technically achievable, and when it is achievable, servicing of space-based assets requires complex planning and cost-benefit evaluations.[59] Unscheduled repairs necessitated by failures resulting from counterfeit parts further complicate such evaluations.

Further, the longevity of certain aerospace programs, as well as technological advances in certain types of components used in aerospace products, gives rise to concerns regarding diminishing manufacturing sources and material shortages ("DMSMS"). Various factors, such as low demand for parts in mature programs, may result in obsolescence and the loss of manufacturers or suppliers of components or raw materials used in aerospace products. When such parts are no longer available from the OCM or their authorized suppliers it may become necessary to procure parts from independent distributors or brokers. Purchases of parts from sources other than OCMs or authorized suppliers or aftermarket manufacturers that have legitimately obtained intellectual property rights require additional steps (*e.g.* supplier audits, tests, and inspections) to limit the risk of receiving suspect parts.

[59] *See* GAO, Space Shuttle: Costs for Hubble Servicing Mission and Implementation of Safety Recommendations Not Yet Definitive, Report No. GAO-05-34 (Nov. 2004)(estimating servicing mission for Hubble Space Telescope to range between $1.7 billion to $2.4 billion).

In 2009, in response to concerns regarding the increased volume of counterfeit parts entering the aerospace supply chain, SAE International issued AS5553, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition," to establish a standard protocol for use in the aerospace industry for detection and mitigation of counterfeit electronic parts. SAE AS5553 is intended to supplement requirements of other quality standards, such as SAE AS9100.[60] Both DoD and NASA have recognized the guidance to industry provided by AS5553.[61] However, a one-size fits all, universal adoption of this standard for all DoD procurements may not be appropriate as there are other standards that have been promulgated or are in draft form and should be considered as well.

In addition, while Section 818 would have DoD craft regulations to implement its concerns, DoD might look at other agencies that have already had to face this problem for ideas on problem areas for implementation and potential workarounds. For example, Section 1206 of the NASA Authorization Act of 2010 required NASA to establish counterfeit part identification training for certain employees, implement an internal database of suspected and confirmed counterfeit electronic parts, that includes GIDEP notifications, and deploy a mechanism to report information on suspect and confirmed counterfeit electronic parts to law enforcement agencies, industry associations and other databases. [62] NASA is developing and implementing detailed procedures for the preparation, distribution, investigation, resolution, and closeout of information pertaining to suspect and confirmed counterfeit electronic parts.[63] The Department of Energy ("DOE") also has had laws and regulations in place to address counterfeits in the nuclear industry. *See* Part IV.C.5, *below*.

4. Construction

[60] SAE is in the process of developing similar standards associated with purchasing applicable to distributors of electronic components and laboratories responsible for testing and authenticating parts from distributors. *See draft SAE* AS6081, "Counterfeit Electronic Parts; Avoidance Protocol, Distributors," and SAE AS6171, Test Methods Standard, Counterfeit Electronic Parts. The International Electrotechnical Commission also has developed a Technical Specification, IEC 62668-1, regarding avoiding the use of counterfeit, fraudulent and recycled electronic components in avionics.

[61] *See* NASA Policy Directive (NPD) 8730.2, "NASA Parts Policy," dated Nov. 3, 2008, identifying AS5553 as an applicable document. *See also* DoD Adoption Notice, available at https://assist.daps.dla.mil, stating that SAE AS5553 was adopted by DoD on August 31, 2009.

[62] 42 U.S.C. § 18444.

[63] *See, e.g.,* NPD 8730.2C, dated November 3, 2008, which details NASA's counterfeit parts control plan (Appendix B) as well as requires the Center Safety and Mission Assurance Directors to report suspected counterfeit parts to the NASA Office of Inspector General (OIG), and the Director, Acquisition Integrity Program (AIP); NASA Policy Requirement (NPR) 8735.1B, dated December 28, 2007, which provides the procedures for exchanging data related to suspected counterfeit parts and other safety problem data through GIDEP and NASA advisories.

Although it is difficult to imagine a "counterfeit" building, the construction industry is just as prone to counterfeit parts – particularly with regard to construction materials and electronic building systems – as any other industry. Some of the unique aspects of the construction industry that may make this problem particularly difficult to combat include: the typical division of responsibilities between the designer and the construction contractor, as well as, the high level of subcontracting in construction projects (including to trade contractors and their material suppliers), an extensive use of COTS items, and significant small business subcontractor involvement in construction projects (sometimes driven by high customer small business requirements).

5. Energy

Counterfeit parts have long been a problem in the energy sector. DOE first formally addressed "suspect/counterfeit items" in July 1988, after receiving a U.S. Nuclear Regulatory Commission Notice regarding discoveries of suspect electrical equipment at commercial nuclear facilities. DOE has reported discovering counterfeits of the following items at DOE or National Nuclear Safety Administration ("NNSA") sites: threaded fasteners, including assemblies containing fasteners such as ratchet tie down straps; various electrical components (semiconductors, circuit breakers, current and potential transformers, fuses, resistors, switchgear, overload and protective relays, motor control centers, heaters, motor generator sets, DC power supplies, AC inverters, transmitters, ground fault circuit interrupters ("GFCIs")); piping components (fittings, flanges, valves and valve replacement products, couplings, plugs, spacers, nozzles, pipe supports); preformed metal structures; elastomers (O-rings, seals); spare or replacement kits from other than the OEMs, weld filler material; and diesel generator speed governors and pumps.[64]

DoD may want to avail itself of the knowledge and experience that DOE has gleaned from having to address counterfeit parts issues since 1988, *e.g.*,

- DOE's suspect/counterfeit items ("S/CI") control policies are based on two safety principles: (1) "defense-in-depth"; and (2) "graded approach."[65] "Defense-in-depth" refers to a multi-layered network of controls to prevent introduction of counterfeit parts, a network that encompasses "the design, procurement, construction, operation, maintenance, and modification processes at DOE/NNSA sites and facilities."[66] The "graded approach" describes a risk-based approach to the contractor's focus of its anti-counterfeiting efforts, with contractors directed to "focus their resources and priorities on those safety systems and mission critical facilities, including critical load paths of lifting equipment, where the introduction of [suspect/counterfeit items] would have

[64] Department of Energy Guide ("DOE G") 414.1-3, "Suspect/Counterfeit Items Guide for Use with 10 CFR 830 Subpart A, Quality Assurance Requirements, and DOE O 414.1B, *Quality Assurance*," November 3, 2004, at ¶ 3.4.
[65] *Id.*, ¶ 3.3.
[66] *Id.*

the greatest potential for creating unsafe conditions."[67] Notably, DOE's "graded approach" to counterfeit prevention sanctions the type of risk-based approach by the contractor to counterfeit detection and prevention that many defense industry sources have advocated DoD permit in the regulations to be imposed on defense contractors under Section 818.

- DOE's policies require that contractors acquire items subject to counterfeiting concerns or known to have been counterfeited in the past from "approved suppliers," a requirement similar to Section 818's mandate that DoD and its contractors/subcontractors acquire electronic parts from OMs, their authorized dealers, or from "trusted suppliers."[68] One step DOE has taken that might prove useful to DoD in establishing the "trusted supplier" requirements under Section 818 is the development of a contractor-accessible database of supplier quality information that would minimize duplicative contractor evaluations of suppliers and relieve suppliers of the need for redundant evaluations by multiple customers. DOE describes the DOE Contractors Supplier Quality Information Group ("SQIG") as a DOE/NNSA-wide cooperative that maintains a common supplier database of evaluated suppliers, accessible to members of the cooperative.[69] Establishing a contractor-accessible database that identifies suppliers whose anti-counterfeiting processes have been evaluated/audited and who have been verified as "trusted suppliers" for designated parts could reduce the costs that might otherwise be passed onto DoD in the form of supplier audit/verification costs incurred by multiple defense contractors qualifying the same supplier as a "trusted source."

6. Medical

Much of the focus on counterfeiting in the medical industry centers on combating the counterfeiting of pharmaceuticals and medical devices. Domestically, the Federal Government has fought counterfeiting of pharmaceuticals largely through attempts to deploy track-and-trace or other authentication technologies, such as basic pedigree/chain of custody obligations.

Section 913 of the FDAA Act created a new Section 505D of the FD&C Act titled "Pharmaceutical Safety."[70] Section 505D directs the Food and Drug Administration ("FDA") to develop new standards for pharmaceutical safety by identifying and validating effective technologies to secure the drug supply chain against counterfeit, diverted, subpotent, substandard, adulterated, misbranded, or expired drugs.[71] Congress specifically directed the FDA, in adopting these new standards, to address "promising technologies," including "radio frequency identification technology," "nanotechnology," "encryption technologies," and "other track-and-trace or authentication technologies."[72] Thus, Congress has charted a course for the FDA's counterfeit prevention strategy that focuses on track-and-trace or other

[67] *Id.*
[68] *Id.*, ¶ 4.1.2.
[69] *Id.*
[70] 21 U.S.C. § 353e.
[71] 21 U.S.C. § 353e(a).
[72] 21 U.S.C. § 355e(b)(3).

authentication technologies that would allow a downstream customer to validate the authenticity of drugs received and identify (and eliminate) counterfeit drugs.[73]

It remains to be seen whether the types of track-and-trace or authentication technologies being explored in the prescription drug arena represent practical options to combat counterfeiting of defense supply chain parts and components. The adoption of track-and-trace or "pedigree" requirements for defense parts would be difficult, if not impossible, to implement to address potential counterfeiting of parts that are already out-of-production and available only through "unauthorized" sources (*i.e.,* not the original manufacturer or one of its authorized dealers), with no practical means of developing a "pedigree" for parts currently held by such sources. A track-and-trace, unique identifier, or "pedigree" option may also be difficult or prohibitively expensive to impose on the types of electronic components that are of the greatest counterfeiting concern to DoD, and the security of such a system would depend on how easily the information could be falsified or mimicked by counterfeiters.

7. International

There are multiple issues that should be specifically considered with regard to the manner and ability to implement Section 818 requirements with regard to international sales and contracting, *e.g.,* conflicting international laws regarding dissemination of information, ability to quarantine goods, evaluation of suspect goods, investigations of international activities, and GIDEP reporting restrictions with regard to international matters outside of Canada and the United States.

8. Small Business

DoD also should to work with Industry to address the problems of compliance with Section 818 requirements as they impact small business. For example, a significant portion of the independent distributor link in the supply chain may include small businesses. The costs associated with Section 818 compliance may impose disproportionate costs on these small businesses. Small businesses may not be able to absorb unallowable costs or provide the level of indemnification that higher-tier contractors or the Government may require. Additionally, large businesses in need of complying with contractual

[73] One such anti-counterfeiting authentication technology being explored by FDA and pharmaceutical manufacturers is the incorporation of physical-chemical identifiers ("PCIDs") into solid oral dosage form drug products. A PCID is "a substance or combination of substances possessing a unique physical or chemical property that unequivocally identifies and authenticates a drug product or dosage form." *Guidance for Industry Incorporation of Physical-Chemical Identifiers into Solid Oral Dosage Form Drug Products for Anticounterfeiting*, FDA Center for Drug Evaluation and Research, October 2011.

obligations to meet socioeconomic goals by contracting with small business may be forced to incur disproportionate costs to vet and subcontract with these small businesses.

V. Conclusion

The Task Force appreciates the opportunity to provide this white paper on implementation of regulations in accordance with Section 818's mandates and looks forward to working with the Government to explore the unique issues and needs posed by the counterfeit parts problem and to assist in the identification of potential best practices to develop workable regulations and compliance programs.