Bloomberg BNA

Federal Contracts Report™



*DOD*

# New DOD Counterfeit Prevention Policy: Resolves Responsibilities Within DOD But Leaves Many Contractor Questions Unresolved

BY ROBERT S. METZGER

Section 818 of the fiscal year 2012 National Defense Authorization Act was enacted at the end of 2011. The statute required DOD, within 180 days of enactment, or by June 28, 2012, to have completed an internal assessment of its policies and systems for the detection and avoidance of counterfeit electronic parts. By the same date, DOD was to issue ''guidance'' on actions that DOD Components can take to ''implement a risk-based approach to minimize the impact of counterfeit electronic parts or suspect counterfeit electronic parts'' on DOD. On March 16, 2012, DOD issued a memorandum signed by Frank Kendall, now Undersecretary of Defense for Acquisition Technology & Logistics (AT&L), entitled ''Overarching DOD Counterfeit Prevention Guidance.'' This (the ''Kendall Guidance'') was understood to be an interim measure.

*Robert S. Metzger, a shareholder with Rogers Joseph O'Donnell, P.C., has written or co-authored three previous articles in Federal Contracts Report on counterfeit parts prevention and supply chain security: (1) An Appraisal of Select Provisions of the FY 2103 National Defense Authorization Act (99 FCR 27, 1/8/13); (2) Counterfeit Electronic Parts: What to Do Before The Regulations (and Regulators) Come? (Part 2) (98 FCR 246, 8/21/12); and (3) Counterfeit Electronic Parts: What to Do Before the Regulations (And Regulators) Come? (Part 1) (97 FCR 647, 6/26/12) (Jeffery M. Chiow, co-author).*

On April 26, 2013 — ten months after the date required by Section 818 — the Pentagon released DOD Instruction (DODI) No. 4140.67, the ''DOD Counterfeit Prevention Policy,'' which responds to the law's direction. DODI 4140.67 expressly supersedes the previous Kendall Guidance.

In some respects, the new DODI disappoints. Most of its volume is in the nature of ''housekeeping'' to clarify assignments and responsibilities within DOD. Rather than offer much in the nature of specific implementation measures, it exhorts various DOD Components to take future actions to enforce the law and more generally improve DOD's ability to prevent entry of counterfeit parts into the defense supply chain and accomplish remediation when this occurs. The new DODI actually omits much of the specific content of the Kendall Guidance and some express requirements of Section 818 are neglected.

But there is more to the DODI than meets the eye. Considering the scope of Section 818, the breadth of the challenge presented by counterfeit materiel, and the multiplicity of DOD Components that have a stake in the subject, the value of role assignments accomplished by the DODI should not be unappreciated. The absence of prescriptive instruction may be deliberate ''forbearance'' as the emphasis on assignments — effectively *delegation* — may presage ''adaptive'' application of high level objectives by DOD Components. Moreover,

the DODI arrives just before new DFARS and FAR procurement regulations that will govern industry.[1]

**What the DODI Does — its 'Purpose.'** DODI 4140.67 establishes DOD's policy and assigns responsibilities necessary to prevent the introduction of ''counterfeit material'' at ''any level'' of the DOD supply chain. The DODI extends beyond electronic parts (the focus of Section 818) to all ''*materiel*,'' which is defined very broadly, applying to system components and subcomponents as well as to software and information and communications technology (ICT). The new DODI addresses anti-counterfeit measures for weapon systems as well as information systems. That counterfeit materiel avoidance policy now extends outside electronic parts and specifically to both software and ICT is a further indication of DOD's emphasis on areas where cyber security and information assurance concerns interact with counterfeit parts prevention.[2] Going beyond Section 818, which applied to electronic parts and large government contractors, the new DODI applies to any form of at-risk materiel and ''at any level of the DOD supply chain.''

**Applicability of the New DODI.** DODI 4140.67 affects many DOD Components. It applies to ''all phases of materiel management,'' recognizing that supply chain security has implications for early-stage activities, such as requirements definition and system design, as well as end-stage processes, such as phase-out, retirement and materiel disposition. The very breadth of the supply chain, so understood, may help to understand why the DODI appears to be short on particulars and long on encouragement. Practically, the imposition of supply chain security measures, and application of risk-based management principles, is context-dependent. It is a positive attribute that the DODI does not attempt to impose overarching ''rules'' that may be well-intended but fit poorly to particular circumstances.

The new DODI applies not only to acquisition but also to related functions such as sustainment. Section 818 required DOD to conduct a self-assessment of its acquisition policies and systems for the detection and avoidance of counterfeit electronic parts. The DODI goes beyond that to encompass many functions before and after the acquisition process, and is concerned with any at-risk materiel, not just electronic parts.

**Key Features of the New DODI.** In enacting Section 818, Congress instructed DOD to improve its acquisition practices and to issue new guidance to implement a ''risk-based approach'' to minimize the impact of counterfeit electronic parts.[3] The new DODI follows this instruction, to a point. The DODI expressly recognizes that the risk of counterfeit parts cannot be eliminated entirely. DOD's policy is to ''[n]ot knowingly procure counterfeit materiel.'' DOD is to employ:

> a risk-based approach to *reduce* the frequency and *impact* of counterfeit materiel acquisition within DOD acquisition systems and DOD life-cycle sustainment processes . . .

(Emphasis added.) While *elimination* is a goal of all responsible actors in the DOD supply chain (public and private), DOD thus has adopted a core proposition that focuses efforts where the risk is greatest in order to minimize the likelihood of a counterfeit incursion and mitigate the impact should such an ''escape'' occur. It is hoped that the same principles will be present in the upcoming DFARS regulations to implement Section 818. For industry as well as government, a cost-effective balance must be found between prevention efforts and their costs, and between such efforts and their effect on military readiness and responsiveness of the industrial base.

Similarly, other features of the DODI articulate sound principles that have broad relevance but necessarily must be tailored when applied. These include:

- Apply prevention and early detection procedures as the primary strategy to eliminate counterfeit materiel within DOD;
- Strengthen the oversight and surveillance procedures for critical materiel;
- Document all occurrences of suspect and confirmed counterfeit materiel in the appropriate reporting systems including GIDEP;
- Make information about counterfeiting accessible at all levels of the DOD supply chain;
- Investigate, analyze and assess all cases of suspected counterfeit materiel.

These principles apply to contractor organizations, of course, but the challenge will be translation to fit the specifics that differ for each contractor. The proposition of ''risk-based methodologies'' is easy to embrace in principle, but difficult and complex to apply. It also implies acceptance of some level of risk. Hence, DOD should not apply a penalty regime against contractors who have acted responsibly but experience a counterfeit escape nonetheless. As to itself, the DODI aims for DOD not to eliminate but to *reduce* the frequency and impact of counterfeit materiel and emphasizes prevention and detection to *minimize* the presence of counter-

[1] Section 818(e)(1) required DOD, not more than 270 days after the date of enactment, or September 27, 2012, of this Act, to ''implement a program to enhance contractor detection and avoidance of counterfeit electronic parts.'' Completion of the regulatory response is thus overdue. As of this writing, there are at least four pending rulemaking cases that concern efforts to defeat counterfeit materiel: DFARS Case 2012-D055 (Detection and Avoidance of Counterfeit Electronic Parts) (cleared by OIRA and reportedly nearing publication); DFARS Case 2012-DO50 (Supply Chain Risk) (in review at OIRA); DFARS Case 2012-D042 (Business Systems Compliance) (under consideration at DAR Council); and FAR Case 2013-002 (Expanded Reporting of Nonconforming Supplies) (DAR staff has completed draft rule). DFARS Case DO55 is to be the principal rule implementing Section 818 and is expected to be issued as a preliminary rule for comment. Case D050 would implement Section 806 of the FY2011 NDAA which allows for exclusion of suspect suppliers. Case D042 may add counterfeit avoidance policies and procedures to the business systems which defense contractors must maintain to DOD's satisfaction. FAR Case 2013-002 is the vehicle by which the long-awaited instructions will be provided for expanded reporting and utilization of GIDEP.

[2] ''The recent DOD assessment of the security threat posed by China attributes responsibility to the People's Liberation Army for many cyber threats and attacks on U.S. information systems. ''Military and Security Developments Involving the People's Republic of China,'' Annual Report to Congress, Office of the Secretary of Defense (May 2013). Counterfeit parts could act as hosts for cyber security threats that could disrupt operation of critical systems, compromise information integrity or risk exfiltration of controlled data.

[3] Section 818(b)(2).

  FCR ISSN 0014-9063

feit materiel. DOD should not impose a harsh, ''strict liability'' regime upon its contractors where it allows itself to engage, in effect, in ''best efforts.''

As concerns the policy to ''document all occurrences of suspect and confirmed counterfeit materiel,'' the proof will be in the pudding, so to speak, and that will not be served up until release of the new FAR provision to expand contractor reporting of nonconforming supplies.[4] GIDEP will have to improve in terms of accessibility, utilization and reliability.

DODI 4140.67 also seeks to improve access to information within DOD. This is welcome as there is considerable anecdotal evidence that communication within DOD Components has been irregular and incomplete, causing uncertainty and inconsistency in action.

There is an enforcement side to the new DODI as well. DOD now will seek ''restitution'' when cases of counterfeit parts are confirmed. DOD will notify criminal investigative organizations or intelligence authorities as well as those who use suspect and confirmed counterfeit material. ''Restitution'' is defined as the process of ''determining the parties accountable to counterfeiting, the judicial penalties available against the parties accountable, and the financial redress required.'' Read literally, a principal purpose of ''restitution'' is forensic, i.e., finding those responsible and making them accountable. However, as used elsewhere in the new DODI, it is clear that DOD's intentions, for ''restitution,'' are to recover ''costs incurred from critical failures and damages caused by counterfeit materiel.''[5] This should cause contractors concern. Even though the DODI allows that the threat of counterfeit materiel cannot be absolutely eliminated, even with best practices and all due diligence, the measure of damages is potentially very expansive. There is no limitation expressed on the scope of liability that a contractor might face.

For higher tier contractors, this implies potential liability for redress at the system level, where ''restitution'' costs — *if* defined too broadly in the new DFARS regulations — easily could amount to many multiples of the direct cost of the counterfeit materiel that caused a failure. Such contractors may have to include risk premiums in future proposals to DOD. Contractors did not create the risk that counterfeit parts will be offered to satisfy demand for which original sources are not available. Contractors have no more power to absolutely eliminate that risk than does DOD acting for its own purposes. Today, a ''safe harbor'' is available to contractors only where the government furnishes a counterfeit part.[6] This is an inequitable form of risk-shifting. It makes contractors unwilling ''guarantors'' against a risk they did not create and cannot exclude.

Also included as key policies are the objectives to ''align'' DOD anti-counterfeit processes to support supply chain goals for weapon system availability and weapon systems support effectiveness and efficiency. These are laudable goals. How DOD is to measure the costs and value of their achievement, in times of limited budgets and a wary contractor base, is left unsaid.

**Compared to Section 818 and the Kendall Guidance: Missing Pieces.** The DODI can be criticized for its ''shorthand'' approach to the key strategies of ''prevention and early detection.'' DOD should have provided more information on *how* prevention is to be accomplished and *what methods* will be applied for early detection. Section 818 emphasizes *controls on suppliers* as the most important way to protect against counterfeit electronic parts.[7] The new DODI does little to explain how this is to be done or what standards apply.[8]

The reach of the DODI extends to counterfeit *materiel*, whereas Section 818 addressed only counterfeit electronic parts. Several provisions of Section 818 are not addressed specifically by the DODI:

■ Section 818(b)(1) defines counterfeit parts to include ''previously used parts represented as new.'' The definition in the DODI makes no reference to such ''used'' parts.

■ Section 818(b)(2) instructs DOD to implement a ''risk-based approach'' to minimize the impact of counterfeit and suspect counterfeit electronic parts and DOD is to issue guidance to address various functions. Except by assignment of responsibilities, the DODI does not address several of the functions required by the statute – sourcing, specific testing instructions or of the need to quarantine counterfeit parts.

■ Section 818(b)(3) requires DOD to issue guidance on ''remedial'' actions to be taken in the case of a supplier who repeatedly fails to detect and avoid counterfeit parts. In the DODI, ''remediation'' concerns the disposition of counterfeit materiel. There is no discussion of actions to be taken against a supplier and the DODI, unlike the statute, makes no reference to supplier ''due diligence'' or to suspension or debarment.

■ Section 818(c)(2) obligated DOD to issue regulations to make contractors ''responsible for detecting and avoiding'' the use of counterfeit electronic parts. The statute makes the cost of counterfeit parts and of ''rework or corrective action'' unallowable. There is essentially no discussion of these subjects in the DODI beyond the general affirmation that DOD will seek ''restitution'' and to recover ''costs incurred from critical failures and damages caused by counterfeit materiel.'' Nowhere in Section 818 is ''restitution'' mentioned, and the apparent measure of damages that DOD intends to

[4] *See* n.1, *supra*. The new FAR regulation that expands contractor reporting requirements, believed to be nearing release, is expected to be effective upon publication. It will continue to rely upon GIDEP as a principal reporting mechanism, but it is expected that GIDEP will be transformed over time.

[5] DODI 4140.67, at Enclosure 2 (Responsibilities assigned to USD AT&L).

[6] Section 833 of the 2013 NDAA provides a ''safe harbor'' only where counterfeit parts come from the DOD as GFP and the contractor has an operational and approved system of counterfeit parts avoidance and is timely in reporting discovery of a counterfeit or suspect counterfeit electronic part.

[7] *See* 818(c)(3) (Trusted Suppliers).

[8] In the Definitions that accompany the DODI, a ''qualified supplier'' is defined as a ''commercial business that has completed the formal process for requesting, evaluating, and approving the capability of a supplier and has met the qualification requirements stated in the applicable military, federal or non-government specification for testing or other quality assurance demonstration that must be completed by an offeror or before award of a contract.'' This definition refers to ''applicable specifications'' that are not now knowable and ''other quality assurance demonstration'' for which standards have not been established and so it is now unknown what demonstration is sufficient.

recover, as framed in the DODI, is different and potentially much larger than what the law requires.

■ Section 818(c)(3) gives great emphasis to controlling sources of parts supply by use of only ''trusted suppliers.'' The DODI contains no discussion of ''trusted suppliers,'' perhaps because of the considerable confusion that has arisen due to various and divergent uses of the term. Instead, the DODI uses the term ''qualified supplier'' but, as noted, employs a definition that raises at least as many questions as it answers.

■ Section 818(c)(3)(B) specifically requires DOD to establish requirements for contractors to give notice to DOD and to perform additional inspection, testing and authentication where parts are not available from trusted suppliers. The DODI does not discuss this requirement.

■ Section 818(c)(3)(C), similarly, requires DOD to establish ''qualification requirements'' to identify ''trusted suppliers'' – but the DODI says little on this subject other than to assign some qualification responsibilities to ASD(R&E).

■ Section 818(c)(3)(D) authorizes DOD contractors to use ''additional trusted suppliers,'' provided they meet standards and processes that conform to established industry standard. This an area of acute importance to industry, because there remains so much demand for parts where the ideal, original sources are not available — but the DODI is silent on the subject.

Presumably, aspects of Section 818 are omitted from the DODI, as affect contractors, will be included in the forthcoming DFARS regulations. Many of the same actions, or responsibilities, will apply to DOD itself when it acts to purchase parts and assumes responsibility for system sustainment — as it does for many thousands of systems. The DODI would have done a service to the overall cause, inclusive of both government and contractor obligations, to address some of these subjects.

In this respect, the new DODI does less than the Kendall Guidance that it replaces. The Kendall Guidance ensured that program managers would be notified by their suppliers and contractors when critical items were not obtained from the original or authorized sources. This requirement is absent from the DODI. Under the Kendall Guidance, even for components that are not mission-critical, a manager must document risk mitigation plans where there is a counterfeit risk. This is omitted from the new DODI. The Kendall Guidance required DOD to work to identify appropriate industry anti-counterfeiting standards. There is no corresponding obligation in the DODI beyond including identification of ''standardized guidelines for contractors to employ'' among responsibilities assigned to USD(A&T). Where items cannot be obtained from original or authorized sources, the Kendall Guidance requires program managers to establish additional testing and verification requirements. This too is absent from the DODI. The Kendall Guidance explicitly instructs DOD to hold suspect parts until resolution of potential nonconformance is completed — but the DODI contains no instructions as to retention or disposition of counterfeits.

**Assignments to DOD Components.** Responsibilities for counterfeit materiel risk reduction are allocated among multiple DOD functions. USD(AT&L) gets the responsibility to establish an ''integrated DOD policy'' and it appears to have primary policy authority and for interagency coordination. This makes sense, because it is through acquisition methods (RFP requirements, SOW items, contract terms and conditions) that DOD will impose its anti-counterfeit materiel policies on suppliers. However, there remains unavoidable overlap in assignments, reflecting the reality that many DOD organizations possess distinct knowledge and must share responsibility to address counterfeit materiel. For example, under the new DODI, the Acquisition element of OSD (AT&L) is responsible for the ''*policies*'' to address counterfeit materiel and to implement ''acquisition *procedures*'' for these purposes. But Logistics and Materiel Readiness (ASD(L&MR)) is also assigned responsibility for ''DOD *procedures* for the prevention, detection, reporting and disposition of counterfeit materiel in the DOD supply chain.'' It also is to align and maintain ''DOD materiel and maintenance management issuances to implement the policies contained in this instruction.''

The supply chain threat encompasses a breadth of functions as is evident from the DODI's definition of ''supply chain'':

> The linked activities associated with providing materiel from a raw materiel stage to an end user as a finished product or system, including design, manufacturing, production, packaging, handling, storage, transport, mission operation, maintenance, and disposal.

Industry, especially those companies who have design and system engineering cognizance, should be aware that they will need to take counterfeit materiel avoidance into consideration at all phases of development, supply and support activity. The Research and Engineering part of OSD, ASD(R&E), is given important responsibilities that include coordination to ''identify critical materiel,'' defined in terms of mission or function criticality or special safety significance. ASD(R&E) also is to lead incorporation of ''anti-counterfeiting design considerations'' and is to collaborate with other DOD Components ''to establish technical anti-counterfeit qualification criteria for suppliers.'' It is curious that ASD(R&E) was given this last responsibility, when DLA — a unit of Logistics & Materiel Readiness — today has procurement responsibility to support thousands of DOD systems in the field and has many active programs to qualify trusted suppliers and sources.[9] Also notable is that ASD(R&E) is assigned lead responsibility for GIDEP – the principal reporting mechanism for counterfeit materiel that is to be used both by government and industry. From an operational standpoint, GIDEP would seem closer to Logistics & Materiel Readiness than to ASD(R&E).[10]

Responsibility is assigned to the Under Secretary of Defense for Intelligence (USD(I)) to advise AT&L of ''counterfeiting risks'' that may affect weapon system operation and to assist in ''implementation of risk assessment.'' Similarly, the DOD Chief Information Offi-

[9] Within the ASD(L&MR) organization there are multiple offices with specific supply chain security and anti-counterfeit responsibilities. *See* Organization Chart for Office of the Assistant Secretary of Defense, Logistics and Materiel Readiness, available at http://www.acq.osd.mil/log/lmr/org_chart.htm (last accessed May 8, 2013).

[10] ''About GIDEP: Frequently Asked Questions (FAQ),'' available at http://www.gidep.org/about/faq.htm (last accessed May 8, 2013).

  FCR ISSN 0014-9063

cer (DOD CIO) is to help develop and manage ''an integrated strategy for anti-counterfeiting for information systems and information and communications technology'' and is to integrate anti-counterfeiting policy into information assurance.

The roles of USD(I) and the DOD CIO are extremely important, first, to avoid counterfeit parts that may harbor malicious code and, second, to avoid compromise of ''trusted systems and networks'' that could occur if ''hostile counterfeits'' are installed in such systems. This is the point of intersection between concerns about counterfeit electronic parts, information assurance, software assurance and ''anti-tamper'' regimes.

The threat of counterfeit materiel most often arises where criminal actors, motivated by profit, provide fake parts that appear to be acceptable. Usually, these fakes can be detected by greater inspection or will reveal their flaws with greater test. More sophisticated fakes may be hard and expensive to detect, but the greatest harm they pose is functional failure after installation. That the supply chain is vulnerable to such fakes is a function, in part, of supply and demand. Criminals ''naturally'' will seek to provide parts that remain in demand but are no longer available from original sources. (They also can offer lower prices than original sources for parts that remain in production or authorized inventory.) In contrast, counterfeit parts that are ''taints'' are produced for malicious purposes. Their ''authors'' may be far more sophisticated enterprises. They will be very difficult to detect and, at least conceptually, such ''taints'' may be ''clones'' of the authentic part that are engineered to mimic the electrical functionality of the original. The threat of ''taints'' is qualitatively different and potentially the consequences are exponentially worse. The danger is *not* that they will fail but that they will operate (pass as good) *and* perform other, unauthorized and adverse functions. Such parts could be carriers of cyber security threats. At least in theory, a very sophisticated counterfeit electronic part could be engineered by a hostile state or even non-state actor to host disruptive code or to act as a gateway for exfiltration of sensitive or controlled technology. This aspect of the new anti-counterfeiting DODI should be read in conjunction with DODI 5200.44, ''Protection of Mission Critical Functions to Achieve Trusted Systems and Networks,'' issued on November 5, 2012.

Broad assignments are also made to ''DOD Components Heads.'' The Components are to integrate DOD anti-counterfeiting policy into relevant guidance, contract requirements and procedures, and implement these policies across a span of functions ranging from prevention and detection to reporting and restitution. They also are to identify and document ''critical materiel'' and materiel that is ''susceptible to counterfeiting,'' and they are to implement anti-counterfeiting measures that ''balance the risks'' of counterfeit materiel ''with the impact to readiness and costs of the measures.'' Moreover, each DOD Component is to procure ''critical materiel'' from suppliers that ''meet appropriate counterfeit avoidance criteria'' and they are to apply ''additional counterfeit risk management measures'' when such suppliers are not available.

It is prudent to leave to each DOD Component the determination of the critical sensitivities of systems to counterfeit materiel. They, or their suppliers, ought to be in the best position to know. But in the sweeping assignment of all responsibilities to all DOD Components, the new DODI may do a disservice to the importance of counterfeit parts avoidance and the likelihood of successful achievement of that objective. Many and various responsibilities, some extremely complex, are delegated to all DOD Components with seeming indifference to the fact that particular duties are undefined and necessary standards are at best unresolved and at worst non-existent. In these areas, as explained, the Kendall Guidance was more complete.

For example, the responsibility to take ''additional counterfeit risk management measures'' when materiel is not available from preferred suppliers is an empty instruction without some guidance or reference to what actions are ''appropriate'' or sufficient to manage risk. The many assignments to DOD Components, because of their generality, expose questions of what those Components are to *do* actually. A similar problem confronts those who are drafting the Section 818 DFARs regulations to govern contractors, because the translation from high-level principles into specific actions and practices remains largely unchartered.

A positive perspective on the new DODI, however, it that OSD recognizes that the supply chain is both so complex and diverse, as it affects DOD and its many Components, that it is imprudent if not impossible to impose *rules* and only sensible, instead, to assert *objectives*. It is hoped that the same restraint will be present in the upcoming DFARS regulations because the *contractor supply chain* is every bit as complex. The best answers to counterfeit parts avoidance are likely to be developed individually by covered contractors, specifically tailored to their programs and products and sustainment obligations. Attempts to impose ''orthodoxy'' by rule will not work and the experience of failure will be costly.

**Risk-Based Methodologies.** Section 818 gave great emphasis, as noted, to the proposition that a ''risk-based approach'' should be employed to minimize the impact of counterfeit electronic parts or suspect counterfeit electronic parts.[11] Not all actions that could be taken to eliminate counterfeit electronic parts should be taken, because the costs could be too great and there could be unacceptable disruption to the defense industrial base. At many places, the new DODI references risk-based assessment:

- DOD's policy is to employ ''a risk-based approach to reduce the frequency and impact of counterfeit materiel within DOD acquisition systems and DOD life-cycle sustainment processes'';

- USD(AT&L) is to coordinate with DOD Components ''to establish a risk-based approach to identify materiel susceptible to counterfeiting and to procure authentic materiel'';

- ASD(R&E) is to coordinate with DOD Components to ''develop and implement risk-based procedures to identify critical materiel'';

- USD(I) is to provide assistance in ''the implementation of risk assessment''; and

- DOD Components are to ''[d]evelop, establish, and maintain performance metrics to assess the risks posed by counterfeit materiel and monitor the effective-

[11] Section 818(b)(2)

ness and efficiency of anti-counterfeit measures and actions.''

A definition of ''risk-based approach'' is provided:

> An analytical strategy to focus attention on areas or applications where failure will produce higher severity of consequences and trigger impacts to the overall mission objectives and human safety.

This is hardly satisfying, considering the importance given to a ''risk-based approach'' in the statute and in the DODI itself. Nor is it complete or even representative of ''best practices'' as developed and promoted by DOD itself.[12] The DODI definition is limited to the ''consequences'' of risk. While certainly important, other factors contribute at least equally — ''Threat'' and ''Vulnerability.'' A risk-based analysis method has been expressed as the following:

**RISK = F(T x V x C)**

(where Risk is a Function of Threat x Vulnerability x Consequence)

**Threat (T)** looks to whether adverse actors have the capability to produce the counterfeit and the motivation to do so. That motivation may be criminal gain, where the counterfeit is made to answer unfulfilled demand for unavailable parts, or it may reflect hostile state or non-state agent ambitions.

**Vulnerability (V)** considers the need or demand for a particular part and whether there is susceptibility to successful insertion of a counterfeit part into the supply chain. Vulnerability is greater where there is demand for parts that are not available from original sources and where there are few controls to assure their authenticity and low demands on traceability. Vulnerability may be lower if a part is difficult or impossible to fake or if a fake is easily detectable, such as results when advanced Item Unique Identification Detection (IUID) methods are employed.

**Consequences (C)** reflects the damage, measured in terms of cost, schedule, performance, integrity, availability, etc., that would be suffered if there is a quality assurance ''escape'' and a counterfeit enters the supply chain.

DOD and other Executive Branch resources are best informed about Threat, especially units that are charged with intelligence and counter-intelligence functions. Industry needs to be informed about the threat ''vectors'' of counterfeit parts. It will benefit from government dissemination of information that now is being accumulated and organized by DOD Components such as the Defense Security Service and the Defense Logistics Agency. Industry needs to know what types of parts are most susceptible to attempted replication by a counterfeit source. They also need to know *what* are the highest risk sources, *where* they are located and *who* most likely will be employed as intermediaries in the distribution chain. Some information, such as foreign ownership, for example, is available from public data sources. Other information may be available only from classified sources, but a ''risk-based approach'' to counterfeit materiel avoidance should be informed as to Threat, just as it is to be aware of Consequences. This suggests that the government should develop a means to share classified supply chain threat information with its cleared contractors. Counterfeiters are ever more sophisticated and constantly evolving their methods to stay ahead of or outsmart detection methods. The U.S. government is far better informed of the evolving threat than is any private company.

As concerns Vulnerability, information also can be gathered from many sources, including government and industry technical resources. Contractors will possess much of relevant information as to systems they build and support. Materiel management and quality assurance systems can provide data relevant to the vulnerability of particular systems to counterfeits. DLA will have similar data for the many systems that they support. Eventually, much of the challenge of assessing vulnerability to counterfeit materiel will be addressed by information management systems. The government should work with industry to develop and adapt these systems to contractors at different tiers of the supply chain.

**Conclusion.** The new DODI 4140.67 can be credited with taking a ''holistic'' approach to the dynamic and complex problem presented by counterfeit materiel. It certainly is ambitious in its aims and expansive in the assignments made within DOD. It is disappointing if one expected rule-based chapter and verse instruction — but this may be prudent in light of the breadth of functions involved and the diversity of programs, projects and responsibilities that will be affected.

Taking an optimistic view, one can credit OSD with taking an approach to the DODI that is ''receptive'' rather than ''prescriptive'' and which establishes complementary goals, leaving it to responsible departments and Components to fashion their own implementation. If this was the ''logic'' behind the new DODI, one hopes that we will see a corresponding strategy in the soon-to-come DFARS that will apply Section 818 to defense contractors. The best way for DOD to accomplish what it wants from its suppliers will not be to indulge in a rule-driven, penalty regime to enforce counterfeit parts avoidance. DOD should encourage and incentivize best practices. Through informed administration, DOD should encourage a multiplicity of risk-informed, tailored solutions that contractors can and will develop.

---

[12] Considerable work has been performed by the Institute for Defense Analysis (IDA) for DOD on managing counterfeit risk in the Department of Defense. The author has heard IDA presentations at several counterfeit parts avoidance forums and acknowledges that this discussion reflects the work of IDA as understood from these presentations. The application of these principles, as here expressed, is the author's own. This is necessarily a preliminary discussion and the author's views are subject to further refinement and change.

  FCR ISSN 0014-9063