

**Presentation of
December 9, 2014**



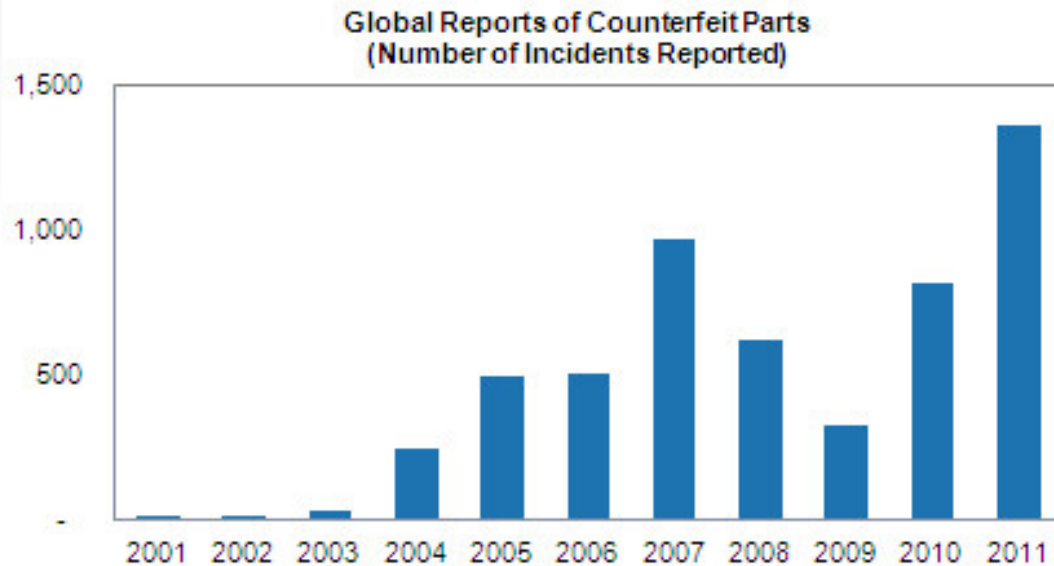
The New DFARS: Considered From a Threat-Based Perspective

Robert S. Metzger
Rogers Joseph O'Donnell, P.C.
750 Ninth Street, N.W., Ste 710
Washington, D.C. 20001
(202) 777-8951
rmetzger@rjo.com www.rjo.com



SASC and Section 818 NDAA FY 2012

SASC's Investigation (leading to 818)



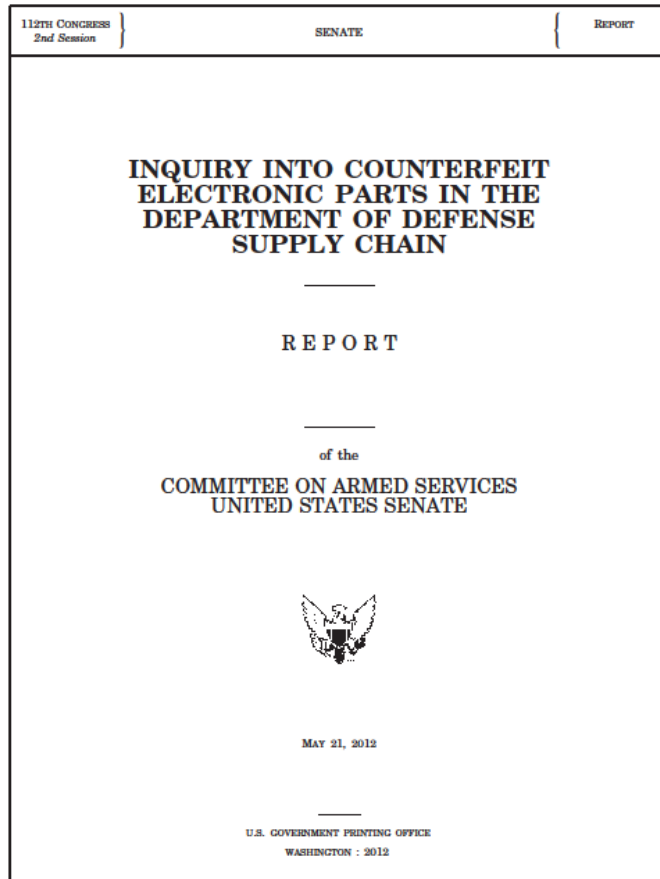
Source: IHS Parts Management

Figures represent ERAI Suspect Counterfeit or High Risk Part Incidents and GIDEP Suspect Counterfeit Alerts for electronic components



Senate Armed Services Committee hearings in 2011 focused attention on the threat and prompted Congress to “legislate supply chain security” through Section 818 of NDAA 2012

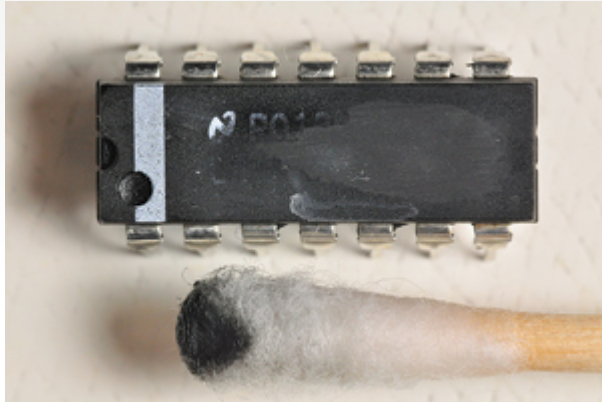
SASC Investigation & Findings



Key SASC findings:

- China is the dominant source country for counterfeit electronic parts;
- The Chinese government has failed to take steps to stop counterfeiting operations;
- DoD lacks knowledge of the scope and impact of counterfeit parts on critical defense systems;
- **The use of counterfeit parts in defense systems can compromise performance, reliability and safety of military personnel;**
- Industry's reliance on unvetted independent distributors results in unacceptable risks;
- Weaknesses in the testing regime for electronic parts creates vulnerabilities; and
- The defense industry routinely failed to report cases of suspect counterfeit parts.

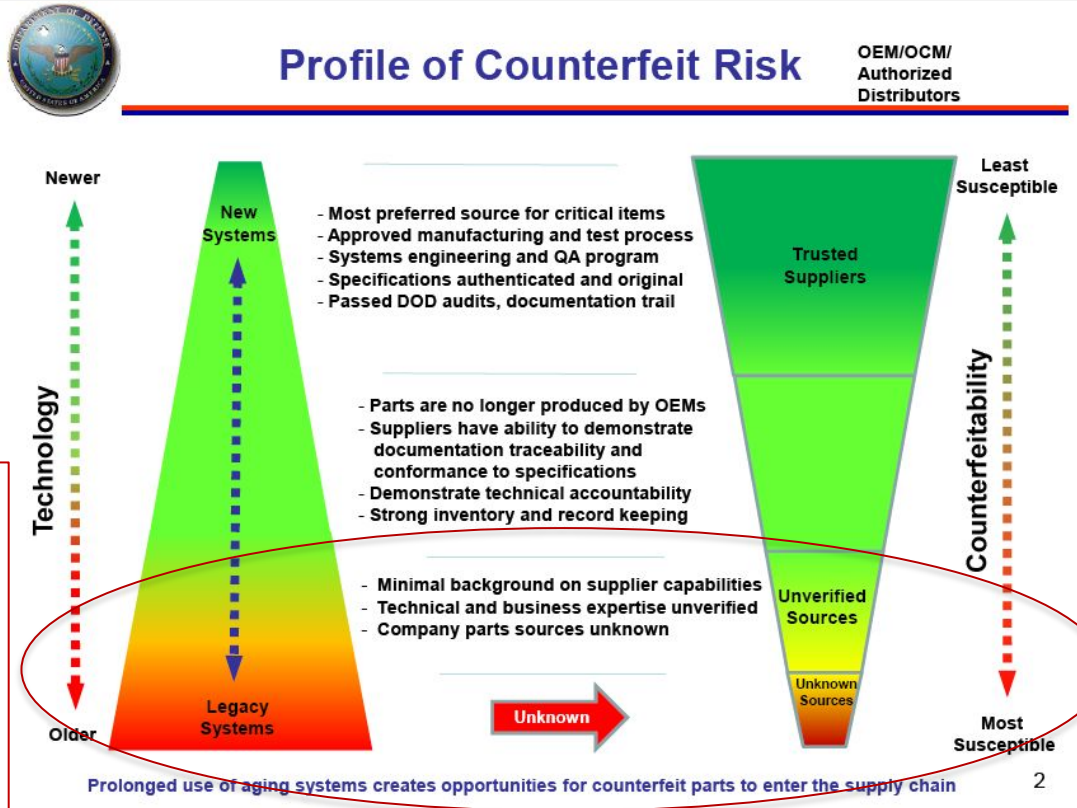
Section 818's Primary Target: *Fakes*



The principal motivation for counterfeit parts, addressed by Section 818, is profit. Bad actors seek to answer demand for scarce parts by offering well-priced fakes that appear genuine -- but are not.

Demand is greatest for parts that are obsolete, out of production and no longer available from OCMs or authorized distributors.

DoD is vulnerable because of the long life of legacy systems that still require support




This risk model is an imperfect fit to the threat of taints to new systems

Section 818 of NDAA FY 2012

Section 818 Operates At Many “Junctions” of the Supply Chain

- Detection
- Exclusion
- Enforcement
- Purchasing Practices
- Inspection & Testing
- Reporting
- Corrective Measures
- Contractor Systems
- Costs & Incentives
- Sanctions

Section 818 Addresses Only Counterfeit *Electronic Parts*



Two Distinct Types of Counterfeit Electronic Parts

Both “Fakes” and “Taints” are “Counterfeit”

The Ordinary (“Fake”) Counterfeit Part:
Substandard or non-functional
Likely to fail in intended environment
Presents risk to operations & reliability
Methods exist to detect (in most cases)
Injury :

- degradation of performance
- diminished reliability
- **potential device/system failure**
- **burden on support & sustainment**
- costs of “remediation”

Typically a counterfeit electronic part contains no active mechanism that can be exploited by an adversary. The defect may be in what is “missing” to assure full functionality and reliability.

But: Some “Fakes” Are Very Sophisticated

“Taint”

“sabotage, maliciously introduce unwanted functions, or otherwise subvert ... a system in order to conduct surveillance or to deny access to, disrupt, or otherwise degrade its reliability or trustworthiness.”

Common Criteria Supply Chain Technical Working Group,
DRAFT “Supply Chain Security Assurance” April 2012,
available at <http://www.commoncriteriaportal.org/>



Unexpected Functionality
Potentially Latent Functions
Vector to induce or exploit cyber attack
Risk of unauthorized extraction
Threat to critical systems and mil ops

Can be very difficult to detect

Sources of the Problem; Nature of the Threat

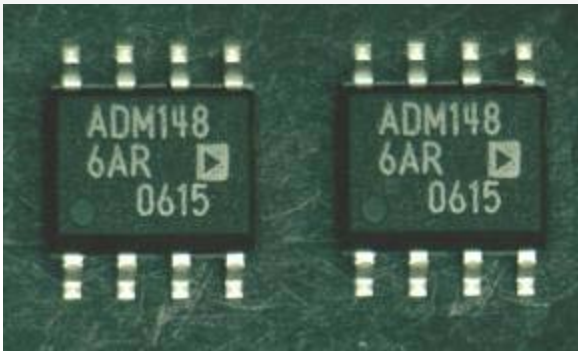
The principal motivation for counterfeit parts, addressed by Section 818, is profit. Bad actors seek to answer demand for scarce parts by offering well-priced fakes that appear genuine -- but are not.



“Malicious” parts may be counterfeit but their threat is different. They may be produced by adversary states or tolerated by state actors. Very sophisticated techniques and resources may be applied. The risk is more than that parts will fail. Threats to operations and to information are posed through hardware, firmware and software, e.g., “Malware,” “Trojan Horse,” “Denial of Service,” Intelligence Extraction, etc.

- *Section 818 will reduce the risk of both counterfeits and malicious parts by emphasizing reliance on trusted suppliers*
- *For national security systems and critical information and communications networks, however, a different and even more demanding response is required*

Convergence of Cyber & Supply Chain Threats



- Examples have been identified of cloned, recent vintage electronic parts
 - From major suppliers
 - Of significant complexity
 - That mimic electrical functionality
- Clones are produced by illegal but highly capable enterprises
- Detection of clones is both costly and difficult – but not impossible

“Recent DoD and U.S. interest in counterfeit parts has resulted in the identification of widespread introduction of counterfeit parts into DoD systems through commercial supply chains. Since many systems use the same processors and those processors are typically built overseas in untrustworthy environments, **the challenge to supply chain management in a cyber- contested environment is significant.**”

The existence of clones points to greater risk that hostile actors will insert harmful code using clones as carriers

DEFENSE SCIENCE BOARD:
Resilient Military Systems and the Advanced Cyber Threat
(January 2013, at p.4)



THE NEW DFARS

79 Fed. Reg. 26092 (May 6, 2014)

Who is Subject to the DFARS?

The DFARS confirm that Sec. 818 is “specifically limited to ‘covered contractors’” and that the initial implementation of the rules “has limited application at the prime contract level to CAS-covered contractors.” 79 Fed. Reg. 26098.

However, the flow down requirement causes the rule to affect all subs – including small businesses

The final rule does exclude set-asides from small business, because CAS does not apply to contracts with small business. “This rule does not apply to small entities as prime contractors.” 79 Fed. Reg. 26105. This limits application of the DFARS when DoD purchases from a small business, but will not affect flow down from covered contractors.

Promulgation comments recognize that small business subcontractors will incur “some costs for complying with prime contractors’ requirements.”

“However, all levels of the supply chain have the potential for introducing counterfeit or suspect-counterfeit electronic items into the end items contracted for under a CAS-covered prime contract. The prime contractor cannot bear all responsibility for preventing the introduction of counterfeit parts. By flowing down the prohibitions against counterfeit and suspect counterfeit electronic items and the requirements for systems to detect such parts to all subcontractors that provide electronic parts or assemblies containing electronic parts (without regard to CAS-coverage of the subcontractor), there will be checks instituted at multiple levels within the supply chain, reducing the opportunities for counterfeit parts to slip through into end items.” 79 Fed. Reg. 26099.

DFARS Obligations on “Covered Contractors”

1) Contractors subject to the rule (“**covered contractors**”) must **establish and maintain systems to detect and avoid counterfeit electronic parts**. The adequacy of these systems will be measured against **twelve criteria**.

2) An emphasis is placed upon practices that will **improve the traceability** of electronic parts so that customers are able to know a part’s history and chain of custody.

3) DoD will oversee and administer the contractor systems as part of “**Contractor Purchasing System Reviews**,” part of the larger program to monitor “business systems” of larger suppliers.

4) Contractors are strongly encouraged to **use original sources (OEMs and OCMs), whenever possible**, but are provided no guidance on how they should qualify other sources if needed parts are not available from the sources considered most trusted.

5) **Notification and additional test and inspection** is required for parts not from the most trusted sources, using “risk-based” methods, though factors and criteria for these methods are not well articulated.

6) Companies must take care to identify both **suspect and confirmed** counterfeit electronic parts and to give **notification** when discovered.

7) Costs of replacing counterfeits are **unallowable** for larger companies that do cost-based contracting with DoD, as are the costs of rework and corrective action.

8) Suspect and confirmed counterfeit electronic parts must be **quarantined and reported** to appropriate authorities and measures must be taken to avoid their being returned into the supply chain.

9) Companies are to improve **training**, make greater use of industry **standards** and keep **informed** on reported counterfeit incidents and on new counterfeiting information and trends.

10) DoD contractors subject to the regulation are required to **flow down** counterfeit detection and avoidance requirements to **all levels** in the supply chain.

Part 202: Definitions

Counterfeit Electronic Part

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

Suspect Counterfeit Electronic Part

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

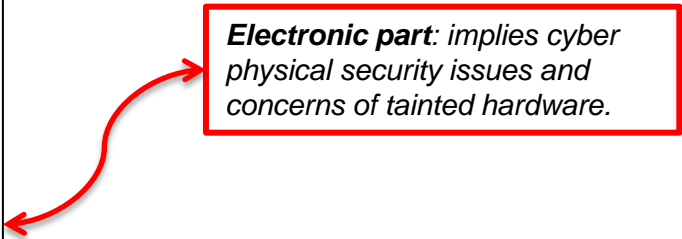
Obsolete Electronic Part

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

Electronic Part

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

Electronic part: implies cyber physical security issues and concerns of tainted hardware.



System Criteria

DFARS 252.246–7007 Contractor
Counterfeit
Electronic Part Detection and
Avoidance
System

Supply Chain Risk Management:

“A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout DoD’s ‘supply chain’ and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).”

DoDI 5200.44 (Nov. 5, 2012)z

(1) Training

The training of personnel.

Contractors have flexibility.

**Training should be tailored for function/
responsibility.**

Refresh needed to recognize new STDs, etc.

**Should a covered contractor confirm subs
conduct training also?**

(2) Inspection and Testing

The inspection and testing of electronic parts, including criteria for acceptance and rejection. Tests and inspections shall be performed in accordance with accepted Government- and industry-recognized techniques. Selection of tests and inspections shall be based on minimizing risk to the Government. Determination of risk shall be based on the assessed probability of receiving a counterfeit electronic part; the probability that the inspection or test selected will detect a counterfeit electronic part; and the potential negative consequences of a counterfeit electronic part being installed (e.g., human safety, mission success) where such consequences are made known to the Contractor.

Publication of **AS-6171** will be important as it provides a hierarchy of test methods and provides a mechanism for risk-based analysis with needed detail.

AS-6171 examines Risk as to the Supplier (R_s), as to the Component (R_c) and as to the Product (R_p) and takes into account Adjustment factors that recognize how each risk area may be mitigated. This is an objective method for contractors to make risk-informed decisions as to what additional measures of test and inspection are appropriate and cost-effective where electronic parts cannot be obtained from preferred, authorized sources such as OCMs and authorized distributors.

However, contractors still will face situations where they do not and cannot know the intended or eventual utilization of a given part. Nor are contractors assured of having relevant knowledge of “threat” relevant to risk of receiving a counterfeit.

This is the closest that the DFARS comes to embracing all elements of the RBA equation. These methods will reduce the risk of “taints” but AS-6171 is not designed or intended to identify alternation to embedded software or firmware.

(3) Proliferation

Processes to abolish counterfeit parts proliferation.

Responsible contractors know they must avoid the “return” of a counterfeit electronic part into the supply chain.

Difficulties arise where a contractor deals with brokers/distributors or test labs who have ownership and possession of parts found suspect or counterfeit. Does the “covered contractor” have control over the disposition?

Also, it may be difficult to establish which party is responsible for reporting the counterfeit.

(4) Traceability

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

Traceability is obviously desirable but this criteria likely will be very difficult to meet for many parts that covered contractors have in inventory and acquire. Today, only a limited class of MIL SPEC (PRF) parts come with end-to-end traceability and these represent only a modest (if not small) fraction of the universe of parts that an aerospace and defense contractor will employ.

While traceability will improve as new demands become regular practices, it will not be possible to satisfy the literal words (“back to the original manufacturer”) for many parts and it would not be cost-effective or practicable only to use parts that have full traceability.

A contractor should be found compliant if it seek all available documentation of pedigree or provenance and considers the extent of documentation when it is necessary to perform a risk-based assessment of a particular source for an electronic part. Certainly, the absence of traceability is a factor (R_C) that may indicate additional inspection and test.

Improving traceability likely will become an important way to reduce supply chain risk both to “fakes” and “taints.”

(5) Use of Suppliers

Use of suppliers that are the original manufacturer, or sources with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources. When parts are not available from any of these sources, use of suppliers that meet applicable counterfeit detection and avoidance system criteria.

A core (and inarguable) principle of the DFARS is that the best way to avoid counterfeits is to procure parts from OCMs, other authorized manufacturers or authorized distributors. However, DoD must support many legacy systems where required parts are obsolete or no longer available from these trusted sources.

The DFARS is short on guidance on how to qualify additional sources when necessary. Contractors may be informed by Standards and best practices to make prudent, risk informed decisions.

Control of sources of supply is the single-most important measure taken to address risk of both “fakes” and “taints.”

(6) Reporting & Quarantining

Reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts. Reporting is required to the Contracting Officer and to the Government-Industry Data Exchange Program (GIDEP) when the Contractor becomes aware of, or has reason to suspect that, any electronic part or end item, component, part, or assembly containing electronic parts purchased by the DoD, or purchased by a Contractor for delivery to, or on behalf of, the DoD, contains counterfeit electronic parts or suspect counterfeit electronic parts. Counterfeit electronic parts and suspect counterfeit electronic parts shall not be returned to the seller or otherwise returned to the supply chain until such time that the parts are determined to be authentic.

The principle that counterfeit and suspect electronic parts should be quarantined is important for several reasons, most important to prevent re-entry, but also to enable appropriate investigation and law enforcement activity. Reporting is a more complex subject.

A pending rule (“Expanded Reporting of Nonconforming Items”) would broadly impose new reporting obligations for non-conforming (and counterfeit) electronic parts and other material. The outcome of this new rule will figure into a compliant reporting mechanism for the purposes of the DFARS. There are a number of complications as concerns reporting. Not all actors in the supply chain have access to GIDEP. Questions also will arise as to which party is responsible to make the report where several tiers of companies are involved in a particular transaction.

Measures should be taken to resolve continuing uncertainty regarding reporting. Coordination with law enforcement and counter-intelligence resources may prove very important to learning from and responding to threats of “tainted” parts.

(7) Identification

Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit.

SAE Standards will figure prominently, along with other industry standards, in selection among compliant methodologies for this purpose.

The definition of “electronic part” in the DFARS “includes any embedded software or firmware.” There is no present Standard or commonly available and accepted method to make this determination.

Costs are another consideration.

(8) Systems to Detect & Avoid

Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts. The Contractor may elect to use current Government- or industry-recognized standards to meet this requirement.

Covered contractors and companies that accept flowdown must develop compliant systems and will be subject to review against the 12 criteria.

The DFARS recognizes the importance of but does not specify particular industry Standards. **None of the Standards today focus on “tainted” parts.**

There will be many challenges. The “systems” requirement is broadly imposed across a highly diverse supply chain that produces and supports an enormous breadth of supplies and functions. DoD has not yet established how it will review and assess the adequacy of contractor systems.

(9) Flowdown

Flowdown of counterfeit detection and avoidance requirements, including applicable system criteria provided herein, to subcontractors at all levels in the supply chain that are responsible for buying or selling electronic parts or assemblies containing electronic parts, or for performing authentication testing.

While a commendable objective, flowdown is beset with serious implementation challenges. Legally, Section 818 and the DFARS apply only to “covered contractors” – about 1,200 companies subject to all of DoD’s Cost Accounting Standards. The flowdown requirement, however, attempts to force those “covered contractors” to obtain the same anti-counterfeit assurance (and system compliance) from all sources in its supply chain – including COTS and commercial item sources and small business. There are 23,000 companies that sell to DoD and many tens of thousands more who supply to those.

Significant supply sources will refuse full flowdown, accept only limited flowdown or offer their own measures as surrogates. DoD’s interests will be served if it interprets and applies the flowdown requirement to mean that its “covered contractors” can use their low-risk, established sources should they decline less than full flowdown.

(10) Keeping Informed

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

This is not a particularly difficult requirement, conceptually, though companies at lower tiers of the supply chain may have some difficulty keeping informed and other companies, for whom aerospace and defense market are not significant, may have insufficient motivation.

A general problem is that counterfeiters continue to “evolve” by using new and more sophisticated techniques. The Government may be the best source of this information – as well as the potentially classified information about threats of “maliciously encoded” or tampered parts – but mechanisms to share such sensitive information today are limited.

There are many “open sources” of data potentially relevant to supplier and device risk analysis; DoD could aid its own cause by leading an effort to organize that information and utilize real-time data analysis.

(11) Screening GIDEP & Other Reports

Process for screening GIDEP reports and other credible sources of counterfeiting information to avoid the purchase or use of counterfeit electronic parts.

Conceptually, this is not an objectionable requirement, but as applied through flowdown to lower tier companies, and to commercial sources and COTS suppliers, it likely will be problematic.

TBD is how to identify and rapidly exploit various government and private databases (e.g., ERAI), and how to resolve potential inconsistencies in reported info. Also unresolved is how to make prudent use of “all source” intelligence information to protect the supply chain while preserving sources and methods.

Looking ahead, data analytics should be used to rapidly process information to “adjudicate” source risks. How will the many sources of data be aggregated, vetted and made accessible?

(12) Control of Obsolete Parts

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

There are many DoD programs (e.g., PPP, DMSMS) and company initiatives to deal with obsolescence, as matters of design, sustainment, engineering and purchasing practices.

However, the value of this 12th criteria is only prospective and it does nothing to help industry deal with the present and very real problem of how to satisfy continuing requirements for parts that already are obsolete or out of production.

A related issue is how to treat inventory that was accumulated before these new rules came in force.

However, it is also true that a robust supply chain that is both resistant to counterfeit attack and resilient in the event of an attack requires attention during the design phase and care to avoid vulnerability that occurs due to diminished sources of supply or materials.

CONCLUSION

Applying “Risk-Based Analysis” to the DFARS

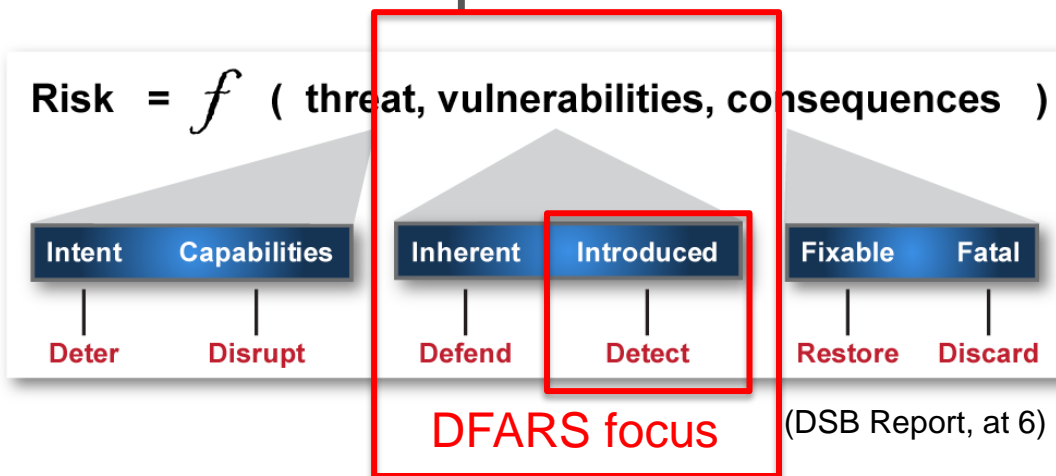
$$R = F(T \times V \times C)$$

R = Risk

T = Threat

V = Vulnerability

C = Consequence



- The DFARS focuses largely on supply chain vulnerability rather than on threats or remediation of consequences.
- Key DFARS attributes are narrowing sources and risk-based test and inspection.
- The DFARS should improve DoD’s protection against the “ordinary” counterfeit.
- Different, more rigorous and threat-informed measures will be needed to deal with taints.
- These special methods should focus on mission critical systems.

Speaker: Robert S. Metzger



Robert S. Metzger received his B.A. from Middlebury College and is a graduate of Georgetown University Law Center, where he was an Editor of the *Georgetown Law Journal*. He was a Research Fellow, Center for Science & International Affairs, Harvard Kennedy School of Government.

Mr. Metzger is the head of the Washington, D.C. office of Rogers Joseph O'Donnell, P.C. A member of the International Institute for Strategic Studies (IISS), he has published on security topics in *International Security*, the *Journal of Strategic Studies* and *Indian Defence Review*. He is the Vice-Chair of the Software and Supply Chain Assurance Working Group of the IT Alliance for Sector (ITAPs), a unit of the Information Technology Industry Council, and also is the Vice-Chair of the Supply Chain Assurance Committee of TechAmerica, both leading U.S. trade associations. He is ranked in 2014 *Chambers USA* as a top Government Contracts lawyer (national).

Rogers Joseph O'Donnell, a boutique law firm that has specialized in public contract matters for 33 years, is ranked in "Band 2" by the 2014 *Chambers USA* – the only boutique among the nine highest ranked firms. Mr. Metzger advises leading US and international companies on public contract compliance challenges.

SELECTED EXTERNAL PUBLICATIONS

available at <http://www.rjo.com/metzger.html>

- "View From RJO: A Standards-Based Way to Avoid Counterfeit Electronic Parts," *Federal Contracts Report*, Nov. 4, 2014
- "You Don't Have to Report Counterfeits to DoD IG," *Law360*, Oct. 6, 2014
- "New Rule Addresses Supply Chain Assurance," *National Defense* (NDIA), Oct. 2014
- "Making the Best of the Final DFARS re Counterfeit Parts," ERAI *Insights* Newsletter, Q2 2014
- "Convergence of Counterfeit and Cyber Threats: Understanding New Rules on Supply Chain Risk," *Federal Contracts Report*, Feb. 18, 2014
- "Counterfeit Electronic Parts: What to Do Before the Regulations (And Regulators) Come?," *Federal Contracts Report*, Jun. 21, 2012 (with Jeff Chiow)
- "Legislating Supply Chain Assurance: Examination of Section 818 of the FY 2012 NDAA," *The Procurement Lawyer*, Vol. 47, No. 4, Summer 2012 (with Jeff Chiow)