DoD's New Supply Chain Measures:
The Counterfeit Prevention Policy (DoDI 4140.67)
Proposed DFAR (Detection & Avoidance of Counterfeit Electronic Parts)

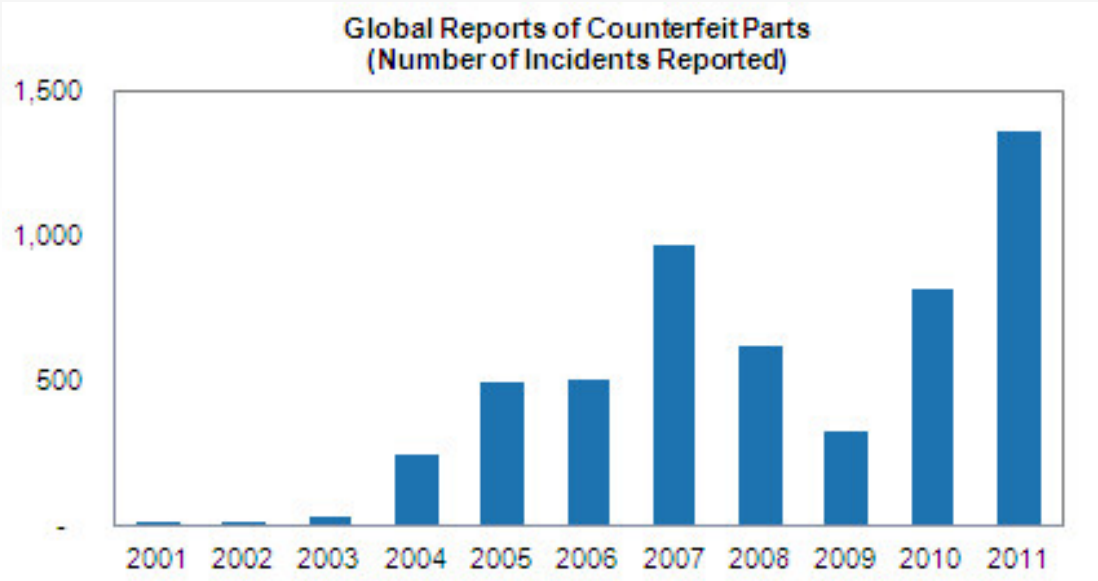
June 25, 2013

SMTA/CALCE Symposium – College Park, MD

Robert S. Metzger
750 Ninth Street, N.W., Ste 710
Washington, D.C. 20001
rmetzger@rjo.com www.rjo.com

A Brief History

Counterfeits: A Growing Threat



Source: IHS Parts Management
Figures represent ERAI Suspect Counterfeit or High Risk Part Incidents and GIDEP Suspect Counterfeit Alerts for electronic components

The 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

Counterfeit Parts: Timeline

- 2008
  - Inside the Air Force
  - Business Week
  - DoJ Prosecutions
  - PRO IP Act
- 2009
  - NASA comments to HEC
  - DoJ Prosecutions
- 2010
  - Dept. of Commerce, BIS Study
  - IPEC Working Group Formed
  - Boeing/L-3 Comm./Raytheon
  - GAO Report: DoD Leverage
  - DoJ Prosecutions
  - **2011 NDAA (Section 806)**
- 2011
  - Dept. of Commerce, Telecom
  - DoD MIBP S2T2 Review
  - **SASC Investigation & Hearing**
  - **2012 NDAA (Section 818)**
- 2012
  - GAO Report: Internet Fakes
  - **AT&L "Overarching" Memo**
  - SASC Investigation Report
  - House Sel. Comm. Report – Telecom
  - DODI 5200.44 Trusted Sys & Nets
  - **2013 NDAA**
    - § 807 – IUID
    - **§ 833 – GFE Only "Safe Harbor"**
    - § 1603 – National Security Strategy
- 2013
  - Continuing Resolution
  - Cyber EO (2/12/2013)
  - GSA "8(e)" Working Group
  - 2014 NDAA (in the works)
  - Proposed DFAR

What Section 818 Requires

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* and Applies Primarily to DoD Primes and High-Tier Subs

818: Detection, Exclusion & Enforcement

Detection – 818(d), (g)

- Strengthened inspection regime for imported electronic parts
- HHS to establish risk-based methodology for import targeting
- CBP may share unredacted information with copyright holder
- New regulations issued allowing CPB to disclose information appearing on merchandise
- Increased detection authority intended to deter foreign sources from att'g to import counterfeits

Section 818 (d)

(d) INSPECTION PROGRAM.—The Secretary of Homeland Security shall establish and implement a risk-based methodology for the enhanced targeting of electronic parts imported from any country, after consultation with the Secretary of Defense as to sources of counterfeit electronic parts and suspect counterfeit electronic parts in the supply chain for products purchased by the Department of Defense.

Enforcement – 818 (h)

- 18 U.S.C. § 21320 adds a criminal offense for trafficking in military goods 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.
- Offense broadened to include attempts and conspiracy
- 1st offenders face a fine of up to $5M (individuals), $15M (corporations), and up to 20 years in prison
- A "counterfeit" is falsely identified or labeled as meeting a military specification, or intended for use in a military or national security application.

818: Purchasing Practices

Section 818(c)(3)

- The core of the new law is the emphasis on purchase from original manufacturers or their authorized distributors.
- Traceability and documentation of authenticity are highest at the level of OCM and Distributor.
- Where parts are unavailable from OCMs or authorized distributors, "notification" is required as well as "inspection, testing and authentication"

More than any other area, industry has been waiting for guidance on how to establish "**additional** trusted suppliers"

(3) TRUSTED SUPPLIERS.—The revised regulations issued pursuant to paragraph (1) shall—

(A) require that, whenever possible, the Department and Department contractors and subcontractors at all tiers—

(i) 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

(ii) obtain electronic parts that are not in production or currently available in stock from trusted suppliers;

(B) establish requirements for notification of the Department, and inspection, testing, and authentication of electronic parts that the Department or a Department contractor or subcontractor obtains from any source other than a source described in subparagraph (A);

(C) establish qualification requirements, consistent with the requirements of section 2319 of title 10, United States Code, pursuant to which the Department may identify trusted suppliers that have appropriate policies and procedures in place to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts; and (D) authorize Department contractors and subcontractors to identify and use additional trusted suppliers, provided that—

(i) the standards and processes for identifying such trusted suppliers comply with established industry standards;

(ii) the contractor or subcontractor assumes responsibility for the authenticity of parts provided by such suppliers as provided in paragraph (2); and (iii) the selection of such trusted suppliers is subject to review and audit by appropriate Department officials.

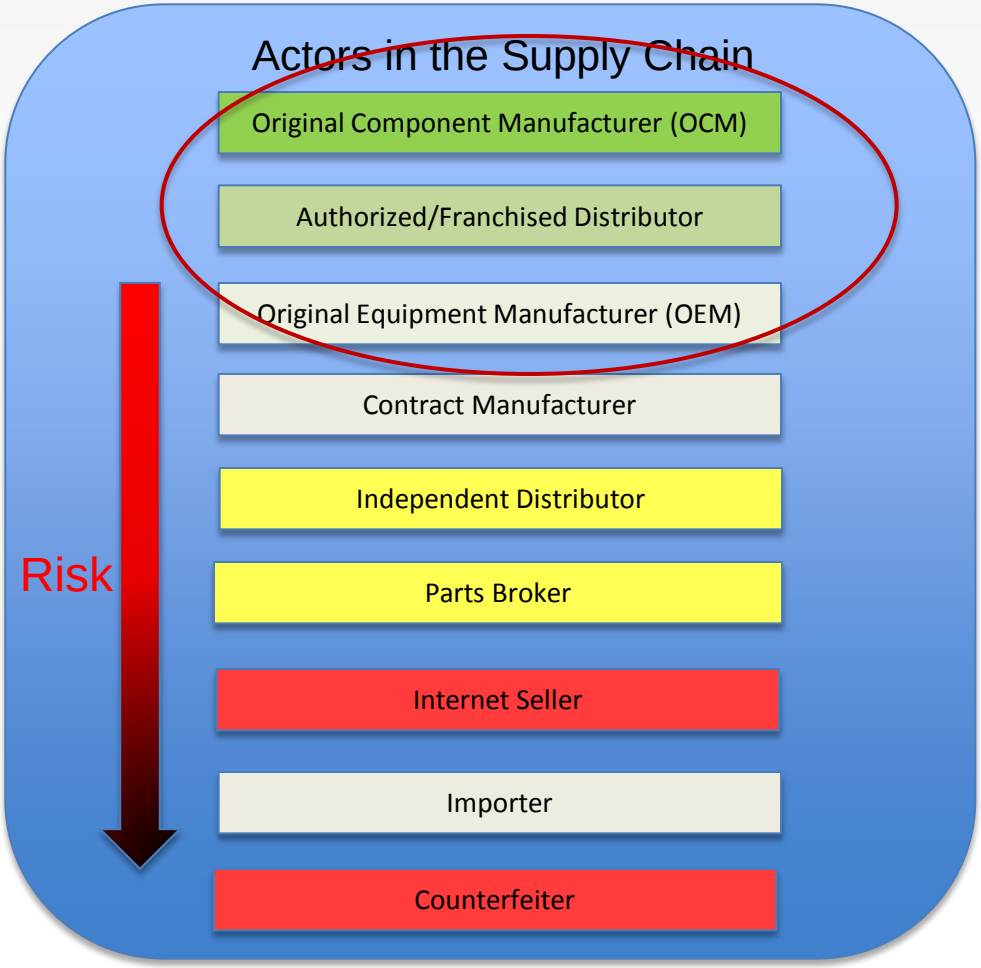
(D) authorize Department contractors and subcontractors to identify and use additional trusted suppliers, provided that—

(i) the standards and processes for identifying such trusted suppliers comply with established industry standards;

(ii) the contractor or subcontractor assumes responsibility for the authenticity of parts provided by such suppliers as provided in paragraph (2); and (iii) the selection of such trusted suppliers is subject to review and audit by appropriate Department officials.

818: Preference for OCMs & Authorized Distributors

- The risk of counterfeit parts is lowest when parts are purchased from OCMs, OEMs and authorized distributors.
- But DoD supports thousands of systems requiring millions of parts that are not available from these (most) trusted suppliers.
- The problem is to decide how to qualify *sources* and *parts* when they cannot be purchased from trusted suppliers.
- Obsolete parts can be redesigned or remanufactured – but at what cost?



818: Contractor Systems for Detection & Avoidance

Section 818 (e)

- Contractor policies and practices must address specific areas:
  - Train personnel
  - Inspect and test electronic parts
  - "Abolish counterfeit parts proliferation"
  - Enable parts traceability
  - Use trusted suppliers
  - Report and quarantine counterfeit (and suspect) parts
  - Identify and rapidly confirm or deny suspect counterfeit parts
  - Design, operate and maintain systems to detect and avoid counterfeit (and suspect) parts
  - Flow down detection and avoidance requirements
- DoD must review and approve (or disapprove) these contractor systems

This is another key area where contractors have awaited guidance

(e) IMPROVEMENT OF CONTRACTOR SYSTEMS FOR DETECTION AND AVOIDANCE OF COUNTERFEIT ELECTRONIC PARTS.—
(1) IN GENERAL.—Not later than 270 days after the date of the enactment of this Act, the Secretary of Defense shall implement a program to enhance contractor detection and avoidance of counterfeit electronic parts.
(2) ELEMENTS.—The program implemented pursuant to paragraph (1) shall—
(A) require covered contractors that supply electronic parts or systems that contain electronic parts to establish policies and procedures to eliminate counterfeit electronic parts from the defense supply chain, which policies and procedures shall address—
(i) the training of personnel;
(ii) the 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) the 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) the design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts; and
(ix) the flow down of counterfeit avoidance and detection requirements to subcontractors; and
(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.

818: Reporting

Applicable to DoD

(b) (4) establish processes for ensuring that Department personnel who become aware of, or have reason to suspect, that any end item, component, part, or material contained in supplies purchased by or for the Department contains counterfeit electronic parts or suspect counterfeit electronic parts provide a report in writing within 60 days to appropriate Government authorities and to the Government-Industry Data Exchange Program (or a similar program designated by the Secretary).

Applicable to Contractors

(c)(4) REPORTING REQUIREMENT.—The revised regulations issued pursuant to paragraph (1) shall require that any Department contractor or subcontractor who becomes aware, or has reason to suspect, that any end item, component, part, or material contained in supplies purchased by the Department, or purchased by a contractor or subcontractor for delivery to, or on behalf of, the Department, contains counterfeit electronic parts or suspect counterfeit electronic parts report in writing within 60 days to appropriate Government authorities and the Government-Industry Data Exchange Program (or a similar program designated by the Secretary).

- Poor reporting proliferates the risk of counterfeit parts and frustrates efforts at detection, avoidance and enforcement.
- The SASC Report showed the inadequacy of the GIDEP system
- Private systems (e.g., ERAI) are useful but not sufficient
- **Both Government and industry need better reporting measures**

818: Sanctions, Correction and Costs

818(b)(3)

DoD is to -

(3) issue or revise guidance applicable to the Department 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 until such time as the supplier has effectively addressed the issues that led to such failures.

The DoD Mandatory Disclosure Program, FAR 52.203-13, has been revised to require contractors to disclose suspected, counterfeit or nonconforming parts discovered during self-policing activities. Failure to disclose is potential cause for suspension, debarment or FCA Liability.

818(c)(2)

(2) CONTRACTOR RESPONSIBILITIES.—The revised regulations issued pursuant to paragraph (1) shall provide that— (A) covered contractors who supply electronic parts or products that include electronic parts 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; and

(B) 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 Department contracts.

What has been accomplished?

New DoD Counterfeit Prevention Policy
DoDI 4140.67
(April 26, 2013)

DoDI 4140.67 – Purpose & Applicability

Issued April 26, 2013 - 10 months after Section 818

- Applies to "counterfeit materiel" not just electronic parts
- Counterfeit avoidance extends to weapon systems as well as information and communications technology (ICT)
- Applies to "all phases of materiel management"
  - Breadth may explain why short on particulars
- Applies both to acquisition and sustainment

The breadth of objective – as well as the "sweep" of the supply chain – may explain why the Instruction does more to "inform" and "assign" than to "instruct" and "specify"

Key Features of DoDI 4140.67

DoD's policy is to "not knowingly procure counterfeit materiel"

- DoD is to employ a "risk-based approach to reduce the frequency and impact of counterfeit materiel acquisition"
- Key strategies include:
  - Prevention and early detection (primary strategy)
  - Strengthen oversight and surveillance for critical materiel
  - Document all occurrences in the appropriate reporting system (GIDEP)
  - Make information about counterfeiting accessible
  - Investigate, analyze and assess all cases
- "Restitution" is sought when counterfeit cases are confirmed
  - determine the accountable parties and the "financial redress required"
- "Align" policies to support system availability & support efficiency and effectiveness

DoDI 4140.67 Compared to Section 818

The DoDI does not:

- Provide guidance on how to implement controls on suppliers
- Answer questions as to qualification of “trusted suppliers” – instead, it uses a term “qualified supplier” (without “how to” instruction)
- Inform as to sourcing, specific testing instructions or quarantine
- Address what “remedial” actions are to be taken against a supplier
- Discuss how DoD will make contractors “responsible for detecting and avoiding” counterfeit electronic parts
- Explain how DoD will determine what costs are unallowable to rework or replace counterfeit parts
- Instruct contractors on how they should deal with obsolete parts
- Specify what additional tests are to be performed when parts cannot be obtained from “trusted suppliers” or what notice is to be given

DoDI 4140.67 – Assignments Within DoD

Responsibilities allocated among many functions:

- *AT&L* is responsible for an "integrated DoD *policy*"
- *Logistics & Materiel Readiness* is responsible for DoD *procedures*
- *Research & Engineering* are given key roles:
  - Identification of critical materiel (mission/function/safety)
  - Technical anti-counterfeit qualification criteria
  - Lead responsibility for reporting (GIDEP)
- *Intelligence* is to advise on "counterfeiting risks" and on "implementation of risk assessment"
- *CIO* is to help develop and manage an "integrated strategy" for information systems ICT and is to integrate anti-counterfeiting policy into information assurance.

The important roles of USD(I) and the CIO point to the intersection between SCRM and cybersecurity

Assignments to DoD Components

The Component Heads have many duties:

- Integrate DoD policy into guidance, contract requirements and procedures
- Implement policies across functions ranging from *prevention and detection* to *reporting and restitution*
- Identify and document "critical materiel" and that "susceptible to counterfeiting"
- "Balance the risks" of counterfeit materiel with the "impact to readiness and costs of the measures"
- Procure "critical materiel" from suppliers that "meet appropriate counterfeit avoidance criteria" *and* apply "additional counterfeit risk management measures" when such suppliers are not available.

DoD components are best informed about the critical sensitivities of their systems to counterfeit materiel.

While much is assigned and little now accomplished, this approach recognizes the myriad of contexts

Risk-Based Methodologies in DoDI 4140.67

Section 818 emphasized use of a "risk-based approach"

- DoD's policy is to employ a RBA to "reduce the frequency and impact of counterfeit materiel" within acquisition & sustainment
- AT&L is to coordinate with Components to establish a RBA to "identify materiel susceptible to counterfeiting" and to procure authentic materiel
- ASD (R&E) is to use RBA in the identification of "critical materiel"
- USD(I) it to assist in implementation of "risk assessment"
- Components are to develop, establish and maintain "performance metrics" to assess risks and efficiency of anti-counterfeit actions

"A risk-based approach" is "an analytical strategy to focus on areas or applications where failure will produce higher severity of consequences and trigger impacts to overall mission objectives and human safety."

Other DoD Takes on "Risk-Based Analysis"

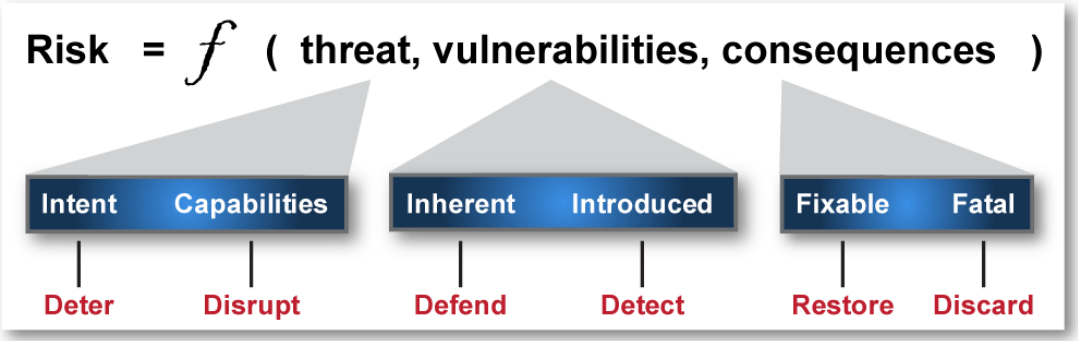
$$R = F(T \times V \times C)$$

R = Risk

T = Threat

V = Vulnerability

C = Consequence



(DSB Report, *Resilient Military Systems and the Advanced Cyber Threat*, January 2013, at 6)

- This principle is being applied across the broad range of supply chain risk management
- Measures are to exclude both "fakes" and "taints" and to prevent data "exfiltration"
- ≥ 90% of CFPs are "fakes" but closest attention is paid to the ≤ 10% that may be hostile
- Hence the emphasis on Trusted Systems & Networks
- New concern about counterfeits as carriers for cyber threat
- Application is context-drive

Proposed DFARS (Case 2012-D055)

(May 16, 2013)

Proposed DFAR (Detection & Avoidance of Counterfeit Electronic Parts)

Issued for comment on May 16, 2013 – 8 months "late"

- Applies only to "electronic parts"
- Problematic definitions (includes)
  - "a new, used, outdated or expired item procured from a legally authorized source that is misrepresented to the end user as meeting the requirements for the intended use."
  - A "suspect" counterfeit part is one "for which visual inspection, testing, or other information provide reason to believe that a part may be a counterfeit part."
- A new contract cost principle makes unallowable the costs of counterfeit or suspect counterfeit parts and the cost of "rework or corrective action"
  - As drafted, the cost principle could apply to all contractors

The Proposed DFAR (II)

- Amends DFARS Subpart 246 (Quality Assurance) to include policy and procedures to implement Section 818.
  - But nothing is said about what constitute acceptable contractor systems to detect and avoid counterfeit electronic parts
- Includes a contract clause that can be used in where the Government is procuring "material containing electronic parts *or services* where the contractor will supply electronic components, parts or materials as part of the service."
- The bulk of the rule focuses on contractor "purchasing systems" and proposes to implement government oversight of contractor counterfeit parts avoidance as part of purchasing system review and approval.

What's Missing - I

- Overall, the proposed rule is sparse
- It provides little detail on implementation and offers slight (or no) guidance on critical contractor concerns
  - Often, it does little more than recite Section 818
  - Emphasis on the Purchasing System does not recognize other contributing functions to counterfeit parts avoidance
  - No guidance is provided on how to select or control sources where a needed part is not available from an original source
  - No information is provided on how to qualify a "trusted supplier" or on additional testing and inspection
  - Nothing is said about the customer's role/responsibility

What's Missing - II

- The proposed DFAR says nothing about contractor use of risk-based assessment
- Nothing is provided that recognizes a balance between objectives and costs/consequences
- No protection or assurance is provided to a contractor who may exert "best efforts"
- Nothing is done to determine applicable industry standards or establish how this will be done
- Contractors cannot identify "best practices" as would mitigate exposure to "strict liability" for a counterfeit

Disingenuous Treatment of Small Business

- The proposed rule claims it will have “negligible” impact on small business – but this is false.
- Section 818 and the rule flow down to all tiers
- Small businesses are least able to absorb additional costs or assume additional liabilities
- A counterfeit sourced from a small business is just as harmful to a system as from a large business – and the prime is liable either way
- Nothing excludes or distinguishes COTS and parts purchased from OCMs

A great disappointment, but not a disaster

- Confronted with 818, industry expected more – and needs more
- The best that can be said for the proposed rule is that it does not attempt to impose "one rule" to fit an infinite number of circumstances
- It may indicate DoD is willing to let industry lead and accommodate many different acceptable outcomes
- But on certain key issues – especially, how to answer demand for obsolete and unavailable parts, where the counterfeit risk is greatest – the rule strikes out

Net Assessment

818 Rulemaking is *Very* Difficult – and will take time

- Threat Characterization: "Fakes" vs. "Taints"?
- Resolving definitions of "counterfeit" and "suspect" parts
- How to define and implement a "Risk-Based Approach"
- Reconciling new rules to a global, commercial supply chain
- Uncertain choices where "trusted suppliers" are not available
- Risk of overreaching rules and overzealous enforcement
- Overlapping and evolving standards and best practices
- Legal and operational issues with an expanded GIDEP
- Industrial base concerns – COTS, small business
- Concern over the "$1B 8086 chip"
- Potentially substantial cost and legal consequences
- "Context sensitivity" of supply chain risk management
- An incentive or penalty-driven regime?

Speaker Biography – Bob 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.

For the ABA Section on International Law, he serves as a Vice-Chair, Aerospace & Defense Industries Committee, and as a Member of the Steering Group of the India Committee. Mr. Metzger is a member of the International Institute for Strategic Studies (IISS), London. Academic publications on international security topics include articles in *International Security*, the *Journal of Strategic Studies* and *Indian Defence Review*. Mr. Metzger is Co-Chair of the TechAmerica Supply Chain Subcommittee.

Mr. Metzger advises leading US and international companies on key public contract compliance challenges and in strategic business pursuits.

SELECTED EXTERNAL PUBLICATIONS
available at http://www.rjo.com/metzger.html

- "DoD Counterfeit Parts Rule – So Little After So Long," *Law360* , June 5, 2013
- "New DOD Counterfeit Prevention Policy: Resolves Responsibilities Within DOD But Leaves Many Contractor Questions Unresolved," (PDF) *Federal Contracts Report*,, May 15, 2013,
- "An Appraisal of Select Provisions of the FY 2103 National Defense Authorization Act," *Federal Contracts Report*, January 8, 2013
- "Counterfeit Electronic Parts: What to Do Before The Regulations (and Regulators) Come? (Part 2)," *Federal Contracts Report*, August 21, 2012
- "Counterfeit Electronic Parts: What to Do Before the Regulations (And Regulators) Come? (Part 1)," *Federal Contracts Report*,, June 21, 2012
- "Legislating Supply Chain Assurance: Examination of Section 818 of the FY 2012 NDAA", *The Procurement Lawyer*, Vol. 47, No. 4 (co-authored by Jeffrey Chiow)

About RJO -- GOVERNMENT CONTRACTS

- San Francisco (1981)
- Washington, DC (2011)
- Chambers USA
  - GovCon Tier 2
- 17 GovCon Attorneys
- Experience across the spectrum
- Impressive clients
- Enterprise-critical assignments
- Thought leadership
- Cleared attorneys, SCI capable