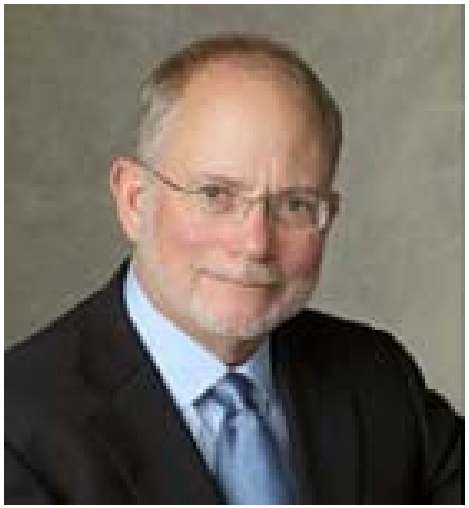
GAINING MOMENTUM 2013

9:00 – 9:45 AM



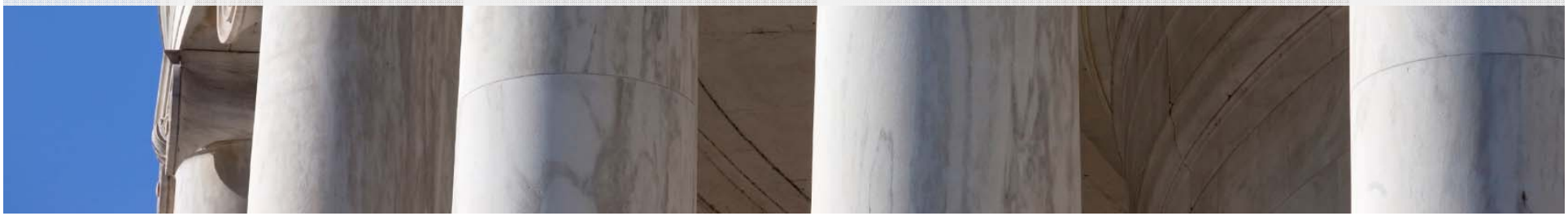
Robert Metzger
Rogers Joseph O'Donnell PC

Supply Chain Security: Reducing Threats to Critical Systems

Supply Chain Security:
Reducing Threats to Critical Systems

April 18, 2013 – General Session

ERAI EXECUTIVE CONFERENCE – ORLANDO, FL



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

• Different but related threats

"Counterfeit"

"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."

DoD "Overarching Guidance" 3/16/2012

"identity or characteristics have been deliberately misrepresented, falsified, or altered without legal right to do so … *suspect* counterfeit: an indication by visual inspection, testing or other information that it may meet the definition of counterfeit material"

DoDI 4140 December 2011

"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

Potential for Unauthorized Extraction

Quality or Reliability (substandard)
Authenticity (misrepresentation)

Differences in origin and purposes

Counterfeit Electronic Parts

"The Investigation uncovered overwhelming evidence of large numbers of counterfeit parts making their way **into critical defense systems**. It revealed **failures** by defense contractors and DOD to **report** counterfeit parts and gaps in DOD's knowledge of the scope and impact of such parts on defense systems. The investigation exposed a defense supply chain that relies on hundreds of unvetted independent **distributors** to supply electronic parts for some of our most sensitive defense systems. And, it found that companies in **China** are the primary source of counterfeit electronic parts in the defense supply chain."

SASC Inquiry into Counterfeit Electronic Parts in the Defense Supply Chain (May 2012)

Supply Chain Risk

"The risk that an adversary may sabotage, maliciously introduce unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system so as to surveil, deny, disrupt, or otherwise degrade the function, use, or operation of such system. "

NDAA 2011 § 806
DODI 5200.44 (Nov. 5, 2012)

NDAA 2012 § 818: Detection and Avoidance of Counterfeit Electronic Parts

Section 806: Supplier Exclusion (2011)

- Definitions:
  - "Covered systems" = "**national security systems**"
    - (information system, including telecommunications system, used for intel, cryptological functions, command & control, and/or integral to weapons system)
  - "Covered items" = **information technology items** bought for inclusion in a covered systems where loss of integrity could result in a **supply chain risk**
  - "Covered procurement" = source selection for a covered system or covered item of supply
- Actions:
  - A **source** may be excluded to reduce supply chain risk (for c/s)
  - Evaluation factors may reflect supply chain risk
  - These decisions may be made (on D&F) without notification on the basis of joint recommendation by USD (AT&L) and CIO acting on "risk assessment" of USD/I of "significant supply chain risk" to covered system

DoD still is working on regulations to implement Section 806. There are problems reconciling the classified source of threat information with the acquisition process – at least for DoD programs not in the classified world. Legally, there are "due process" problems and operationally DoD is concerned about disclosure of vulnerabilities or sensitive information. But NDAA 2013 § 1603 and the FY 2013 CR show Congress remains very concerned that certain sources be excluded from TS&Ns.

Section 818: Counterfeit Electronic Parts

NDAA 2012 Section 818

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

Congress enacted Section 818 after well publicized SASC hearings exposing both real risks and insufficient vigilance on the part of either government or industry. The law thus is "holistic" in that it operates at many junctions of the supply chain. It will result in diverse and demanding obligations on U.S. and international contractors and their commercial electronics sources.

*The principal threat addressed by Section 818 is that of "counterfeits" which will fail and compromise systems and missions. As its rules are implemented, it will help address the risk of **malicious** parts especially by narrowing sources.*

Section 818: Status Report

Section 818: The Requirement

SEC. 818. DETECTION AND AVOIDANCE OF COUNTERFEIT ELECTRONIC PARTS.

(a) **ASSESSMENT OF DEPARTMENT OF DEFENSE POLICIES AND SYSTEMS**.—The Secretary of Defense shall conduct an assessment of Department of Defense acquisition policies and systems for the detection and avoidance of counterfeit electronic parts.

(b) ACTIONS FOLLOWING ASSESSMENT.—**Not later than 180 days** after the date of the enactment of the Act, the Secretary shall, (a)—

(1) establish Department-wide definitions of the terms ''counterfeit electronic part'' and ''suspect counterfeit electronic part'', which definitions shall include previously used parts represented as new;

(2) issue or revise guidance applicable to Department components engaged in the purchase of electronic parts to implement a **risk-based approach** to minimize the impact of counterfeit electronic parts or suspect counterfeit electronic Parts ….

(c) REGULATIONS.—

(1) IN GENERAL.—**Not later than 270 days** after the date of the enactment of this Act, the Secretary shall revise the Department of Defense Supplement to the **Federal Acquisition Regulation** to address the **detection and avoidance** of counterfeit electronic parts.

Status Report:

- **DoD was to complete its internal assessment by 6/28/2012**
- **DoD released "Overarching Guidance" on Mar. 1, 2012**
- **DoD has been working on a "Counterfeit Parts Policy " since 2011**
- **New Regulations were due by 9/26/2012**
- **DoD Released DODI 5200.44 (Trusted Systems and Networks) on 11/22/2012**
- **There are four "rule-making" cases**
  - **FAR: Expanded Reporting of Non-conforming Supplies**
  - **FAR: Commercial and Govt'l Entity Codes**
  - **DFARS: 2012-DO55 – "Detection and Avoidance of Counterfeit Electronic Parts"**
  - **DFARS: 2012-D050: "Supply Chain Risk" – implementing NDAA 2011 § 806**
- **None of the new contract regulations have been issued. Debate continues.**

The breadth of 818 works for *and* against it …

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

Counterfeit parts are a complex challenge. Statutes are an unwieldy way to deal with such complexity. Many federal interests & agencies are involved. Rivalries exist among agencies with competing agendas. Input from industry has been limited. Legal issues abound. Industrial base and budget constraints are present.

There are *many* "acute" implementation problems

- Threat Characterization: "Fakes" or "Fakes & Taints"?
- Resolving the 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
- Standards and best practices largely remain undetermined
- Very limited "safe harbor" even if best practices are used
- Uncertain industrial base impact
- Potentially substantial cost and legal consequences
- Difficulty to manage GIDEP and other reporting (e.g. ERAI)
- **Risk allocation or "blame shifting"?**

Benefits of delayed action

- No regulations are better than bad regulations
- Early drafts reportedly were potential disasters
- Overly ambitious statute + overbroad implementation + overzealous enforcement = a (very) bad equation
- Concern over the "$1B 8086 chip"
- Recognition of DoD dependency on global sources*
  (* *except* for certain "Trusted Systems & Networks") (and CR 2013 – China exclusion)
- Industry standards are "evolving" not "established"
- Worry about supply chain disruption
- **Follow industry rather than "herd the cats"?**
- **Potential overstatement of the problem?**
- **An incentive or a penalty regime?**

818 Implementation: Questions to consider

- Will new rules be effective on release?
- Who will be DoD's trusted suppliers? Who decides?
- How prescriptive will or should the DFARS rules be?
- What application via FAR to other federal purchases?
- How long will contractors have to implement?
- Are contractors at risk now?
- Who in DoD can or will audit compliance?
- Can and will DoD engineer out obsolescence?
- Can one rule fit the entire supply chain?
- Can there be gradual or pilot implementation?

Smart Thinking: Risk-Based Analysis

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

R = Risk

T = Threat

V = Vulnerability

C = Consequence

- 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

RBA is “context-sensitive”

- Access to threat information (commercial, CI)
- Position in the supply chain
  - DoD “covered contractor”
  - Downstream supplier
  - Component or part vendor or commercial source
- Sources of parts and nature of customer demand
- Critical or high-risk applications
- Internal assets and resources
- Ability to anticipate / respond to obsolescence
- Presence of established standards & practices

Key Implementation Propositions: Sell-Side

1. Assess sources and documentation for inventory
2. Specially examine or discard potentially risky inventory
3. Limit purchasing to known/trusted sources – “whenever possible”
4. Insist upon documentation and traceability; visit and know sources.
5. Develop training for personnel & management
6. Improve incoming inspection & test; establish special test relationships
7. Establish “suspect” counterfeit alert criteria and disposition rules
8. Document new policies and procedures & follow written rules
9. Develop mechanism to assure reporting to ERAI and GIDEP
10. Update purchase order T&Cs to avoid excess contractual/legal risk
11. Never “certify“ or indemnify “not counterfeit” – but disclose work done
12. Quarantine suspect items and self-report if any “escapes” occur
13. Demonstrate adherence to and adoption of industry standards
14. Perform periodic diligence to validate and reinforce compliance

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 advises leading US and international companies on key public contract compliance challenges and in strategic business pursuits. His litigation practice includes representation of companies before administrative agencies as well as civil matters in federal and state courts. His transactional practice includes international projects, joint ventures, direct and FMS sales to foreign governments

SELECTED EXTERNAL PUBLICATIONS

- "Counterfeit Electronic Parts: What to Do Before The Regulations (and Regulators) Come? (Part 2)," *Federal Contracts Report*, Vol. 97, August 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)
- "U.S.-India Defence Cooperation: Towards an Enduring Relationship," *Indian Defence Review*, Vol. 27 (2), April-June 2012
- "A 'Work in Progress' – The Evolving U.S.-India Defense Supply Relationship," Indian Law News (ABA Section of International Law), Vol. 2, Issue 3, Summer 2011 (co-authored by Sanjay Mullick),
- "A Critical Reassessment of the GAO Bid-Protest Mechanism," *Wisconsin Law Review*, Volume 2007, Number 6, 2008 (co-authored by Daniel Lyons)