A Standards-Based Way To Avoid Counterfeit Electronic Parts

Presentation of April 22, 2015

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

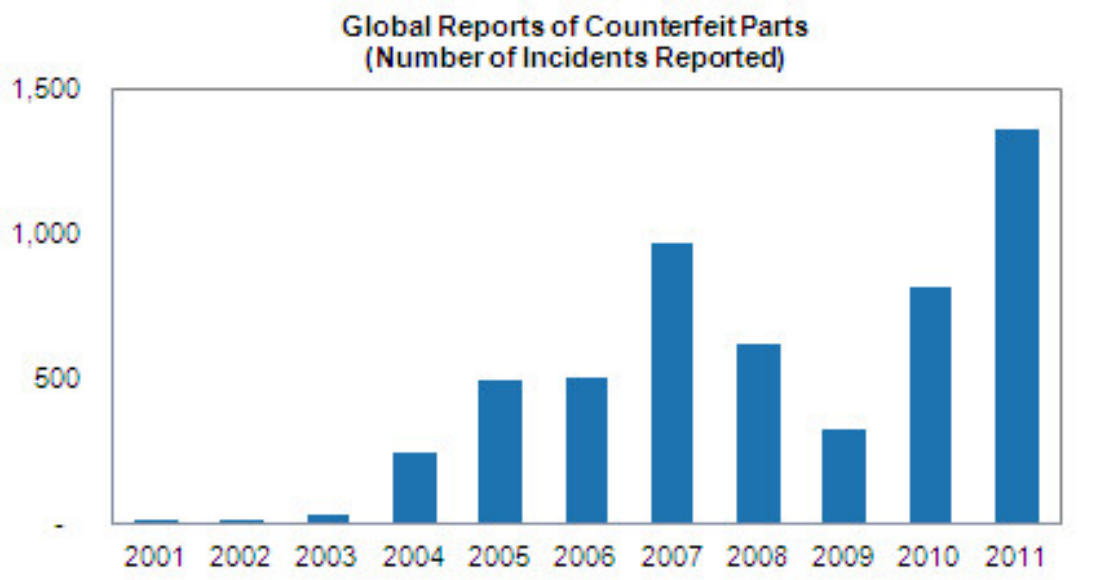
Introduction: where we stand

- The Senate Armed Services Committee exposed the threat of counterfeit electronic parts in 2011 hearings
- Late in 2012, Congress enacted FY 2012 NDAA Section 818
- Final DFARS (May 2014) require "covered contractors" to have systems to "detect and avoid counterfeit electronic parts."
- Industry still is waiting for further regulations on qualification of "additional trusted suppliers"
- And the pending rule on "expanding reporting" is stalled
- Prime contracts (and contractors) now are subject to the DFARS
- Subject companies seek to comply and avoid (or shift) risk

Critical questions remain unresolved

A BRIEF HISTORY

Counterfeits: A Growing Threat

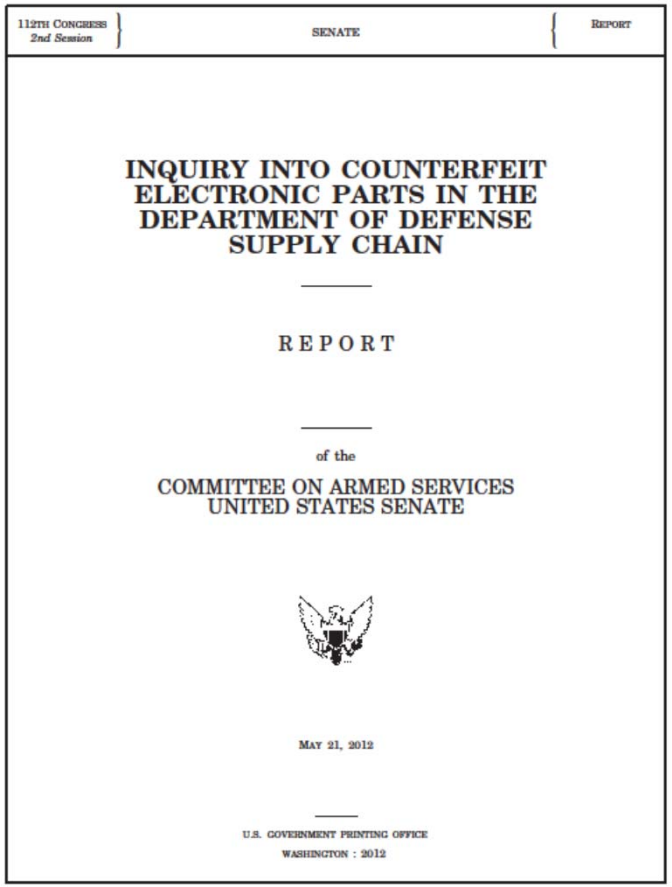


Source: IHS Parts Management
Figures represent ERAI Suspect Counterfeit or High Risk Part Incidents and GIDEP Suspect Counterfeit Alerts for electronic components

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

Current statistics? Unknown

SASC Investigation & Findings



112TH CONGRESS 2nd Session | SENATE | REPORT

INQUIRY INTO COUNTERFEIT ELECTRONIC PARTS IN THE DEPARTMENT OF DEFENSE SUPPLY CHAIN

REPORT

of the

COMMITTEE ON ARMED SERVICES
UNITED STATES SENATE

MAY 21, 2012

U.S. GOVERNMENT PRINTING OFFICE
WASHINGTON : 2012

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.**

Report Card: C

Section 818 of NDAA FY 2012

Applies to "covered contractors who supply electronic parts or products that include electronic parts" 818(c)(2)(A)

Costs of rework or corrective action "required to remedy the **use or inclusion** of counterfeit electronic parts are **not allowable**" 818(c)(2)(B) – not limited to costs on supply

"whenever possible, [DoD] contractors and subcontractors at all tiers" are to obtain electronic parts from trusted suppliers 818(c)(3)(A)

reporting requirement applies to "any Department contractor or subcontractor who becomes aware …" of a counterfeit 818(c)(4)

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

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

1,200 CAS-covered companies are directly subject to the DFARS

Flow down will reach many of the **23,000** other companies that sell to DoD … and **tens of thousands** also in the DoD supply chain

"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: Basic Requirements

1. Improve **training**, make use of industry **standards** and keep **informed**
2. Use **risk-based methods** for notification and **additional test and inspection** for parts not from the most trusted sources
3. Implement processes to **abolish proliferation** of counterfeit parts
4. Improve **traceability**
5. Use **original sources** (OEMs and OCMs), whenever possible
6. Counterfeits must be **quarantined** and **reported**
7. Identify both **suspect and confirmed** counterfeit electronic parts
8. Maintain **systems to detect and avoid counterfeit electronic parts**
9. Counterfeit detection and avoidance must **flow down** to **all levels**
10. Keep **informed** and **screen reports** to avoid buying counterfeits
11. Control **obsolete parts**

Costs to replace counterfeits and for rework are **unallowable;** covered contractors must satisfy "**Contractor Purchasing System Reviews**"

MANY COMPLIANCE QUESTIONS CAN BE ADDRESSED BY USE OF INDUSTRY STANDARDS & BEST PRACTICES

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

(8) 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**.

Why are Standards & Best Practices Important?

- To answer questions government regulators can't or won't
- To provide a common basis for risk assessment "upstream" and "downstream" in the supply chain
- As foundation for dynamic improvement in practices rather than static responses vulnerable to evolving threats
- To facilitate the use of independent accreditation and validation methods that will increase assurance
- To demonstrate sufficient and responsible systems as qualification for new work and to sustain supply relationships
- As answers to challenge should an "escape" or "event" occur
- To respond to situations where purchaser expectations cannot be reconciled with technical, market or financial realities

EXAMPLES:
DRAWN FROM THE DFARS SYSTEM CRITERIA

Adequacy of Systems to Detect & Avoid

DFARS System Criteria (#8)

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.

SAE has produced a series of standards relevant to many supply chain actors, e.g.,

AS5553 ↔ OEMs/Users of Electronics
AS6081 ↔ Independent Distributors of Elec's
AS6496 ↔ Authorized Distributors
AS6171 ↔ Test Methods (for Labs +)
ARP6178 ↔ Risk Assessment of Distributors
AS6301 ↔ Verification for AS6081

Sufficiency of Systems of *Suppliers*

DFARS System Criteria (#9)	
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.	Flowdown is beset with serious implementation challenges. Section 818 and the DFARS apply only to DoD contractors (1,200) companies subject to all of DoD's Cost Accounting Standards. Flowdown, however, makes those "covered contractors" seek the same anti-counterfeit assurance (and system compliance) from all sources in its supply chain – including COTS and commercial item sources and small business. Significant sources have refused full flowdown; others accept only limited flowdown or offer their own measures as surrogates. Even as to suppliers who have anti-counterfeit systems, how can they demonstrate compliance? How can their customers be assured of system adequacy. It is impossible to audit or validate all. A "validate once, use many" approach is necessary. Organizing systems around SAE and similar standards will benefit both purchasers and suppliers – and provide demonstration to oversight authorities.

Qualification of "Other" Suppliers

DFARS Criteria (# 5)	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. To insist upon reverse engineering or contract manufacturing is unaffordable and disruptive of sustainment needs. In many situations, the best answer will be to obtain necessary parts from brokers and distributors and to perform additional test and inspection as indicated by risk assessment. The DFARS offers no real guidance on how to such qualify additional sources when necessary. But Standards – such as AS555A, AS6081 and AS6171 (when released) – will help purchasers make informed decisions and reduce risk.
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.	

Inspection and Testing

DFARS System Criteria (#2)	AS6171 will provide a hierarchy of test methods and provides a mechanism for risk-based analysis with needed detail. It 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. Still, use of AS6171 will provide a normalized basis to assess risk and decide what additional assurance measures are necessary.
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.	

Reporting & Quarantining

DFARS System Criteria #6	
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.	**Counterfeit and suspect electronic parts should be quarantined, to prevent re-entry, and to facilitate investigation and law enforcement.** **Reporting is a complex subject that deserves urgent attention. The DFARS has led to a perception reporting reflects badly on the reporting party. A GIDEP report can have adverse business consequences or even prompt an IG investigation. But when reporting is avoided, customers and other supply chain participants are denied information on counterfeit parts, threat vectors, affected systems, etc.** **GIDEP suffers from limited access and insufficient utility. While voluntary, ERAI plays an important role, focusing on parts, and supporting informed purchasing decisions.** **SAE standards do not offer definitive guidance. AS6081 calls for reporting of "all occurrences" to "customers, applicable Government authorities, Government reporting organizations … [and] industry reporting programs (e.g., ERAI or equivalent." Practical details are missing.**

Traceability

DFARS System Criteria (# 4)

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, while desirable, will be very difficult to meet for many parts now in inventory or available to brokers. Few (MIL SPEC (PRF)) parts have end-to-end traceability.

Traceability will improve as standard OEM practices change. But it is impossible to satisfy the literal words ("back to the original manufacturer") for many parts and it is not cost-effective or practicable to use only parts that have full traceability. A contractor should consider the extent of available documentation when it is necessary to perform a risk-based assessment of a particular source; absence of traceability is a factor (R_C) that may indicate additional inspection and test.

SAE's AS6081 recognizes the practical limitations on traceability; it states, at 4.2.4: the "documented process shall require the retention of records providing supply chain traceability *wherever such traceability exists*." (Emphasis added.)

Identification

DFARS System Criteria (# 7)	DoD is paying increasing attention to the threat of maliciously-encoded or tampered electronic parts. (This is a "cyber-physical" threat.) The DFARS includes "any embedded software or firmware" in the definition of an "electronic part." This suggests an obligation to validate There is no present Standard or commonly available and accepted method to make this determination for most parts. SAE is working, through the G-19A Tampered Subgroup, to create a Test Method to detect embedded malware and hardware Trojans at the electronic piece part level." New technologies are being promoted to enhance testing of large volumes of parts for physical or cyber-physical discrepancies. Standards will emerge on the qualification and use of such new methods.
Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit.	

CONCLUSION

Standards Help Answer Tough Questions

1. **How to demonstrate adequate systems to avoid counterfeit parts?**
2. **How to validate the sufficiency of systems of lower tier suppliers?**
3. **How to qualify suppliers other than OEMs/OCMs?**
4. **When to perform additional test & inspection – and which methods?**
5. **Who reports identified counterfeits or "suspect" parts and how can information exchange be improved?**
6. **How to enable data-driven systems to address risk and inform decisions?**
7. **How can COTS and commercial sources participate in that supply chain?**
8. **Do brokers and distributors have a future role in the supply chain?**
9. **How to reconcile 818 with *continuity* and *affordability*?**

Presenter: 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*. Before practicing law, Bob was a Research Fellow at the Center for Science & International Affairs, Harvard Kennedy School of Government (now "Belfer Center")..

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, a 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

- "Cybersecurity for the Rest of Us: Protecting Federal Information of Civilian Agencies," *Federal Contracts Report*, 103 FCR ___, Mar. 10, 2015
- "DOD's Cybersecurity Initiative - What the Unclassified Controlled Technical Information Rule Informs Public Contractors About the New Minimums in Today's Cyber-Contested Environment, "*Federal Contracts Report*, 102 FCR 744, Dec. 30, 2014
- "A Standards-Based Way to Avoid Counterfeit Electronic Parts," *Federal Contracts Report*, Nov. 4, 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
- "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)