DFARS UPDATE: NDAA 2012 Section 818, Final Rule

Detection and Avoidance of Counterfeit Electronic Parts Overview

Mary Lockhart
Senior Lead Research Engineer
937.528.8690

NEPP Workshop
June 17, 2014
Goddard Spaceflight Center

wyle

The Contractor's Counterfeit Electronic Part Detection and Avoidance System must address:

- The training of personnel;
- The inspection and testing of electronic parts, including criteria for acceptance and rejection;
- Processes to abolish counterfeit parts proliferation;
- Processes for maintaining electronic part traceability;
- Use of suppliers that are the original manufacturer, or sources with the **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;
- The reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts;
- Methodologies to identify suspect counterfeit electronic parts and to rapidly determine if a suspect counterfeit electronic part is, in fact, counterfeit;
- Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts;
- Flow down of counterfeit detection and avoidance requirements;
- Process for keeping continually informed of current counterfeiting information and trends;
- Process for screening the Government-Industry Data Exchange Program (GIDEP) reports and other credible sources of counterfeiting information.
- Control of obsolete electronic parts**.**

Why would you care?

- Stiff first time offender fines! $5M fine (individual), $15M (corporate), up to 20 years in prison
  - *(BTW, you can buy liability insurance for this)*
- System integrates into existing purchasing system
  - If not approved by DoD, potentially disallow entire system
- Your favorite OCM/distributor might not like the flowdown of liability
- Shifting of risk in supply chain requires (thoughtful, different, more, partnering) approaches to test and inventory controls.

Scope

- Requires a counterfeit detection program, avoidance of counterfeit or suspect counterfeit parts, use of trusted suppliers, and requirements to report both counterfeits and suspected counterfeits to government (GIDEP)
- Applies to companies that are subject to Cost Accounting Standards **and their subcontractors**
- Does not apply to small businesses as primes that sell directly to the Government; traceability still required.
  - FFRDCs and UARCs not specifically excluded
  - Does apply if **subcontracting** to a CAS-covered prime
- Limited exception for Government furnished parts, if:
  - Contractor has the required systems in place, and the escape occurred anyway.
  - Timely notice to the Government (60 days)

Definitions

- *Electronic part* means 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**.

- *Obsolete electronic part* means 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**.

- *Suspect counterfeit electronic part* means 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**

Counterfeit parts defined

- The Rule defines “counterfeit electronic part” to mean 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 indication of grade, serial number, lot number, date code, or *performance characteristics.*

Industrial standards do not provide cover

- Methods and technical approaches will need to evolve with the sophistication of the counterfeiters
- Existing standards specifically rejected in the rule making
  -obsolete already, conflicting definitions
- Some counterfeit parts will pass electrical tests of AS6081
- The test scheme must account for the risk of the source and the application.
  - 100% test not feasible nor desirable
- Excerpted: “With regard to mission-critical electronic parts and electronic parts that could impact human safety, DoD does have a zero-tolerance policy”

Use trusted suppliers and impact risk analysis

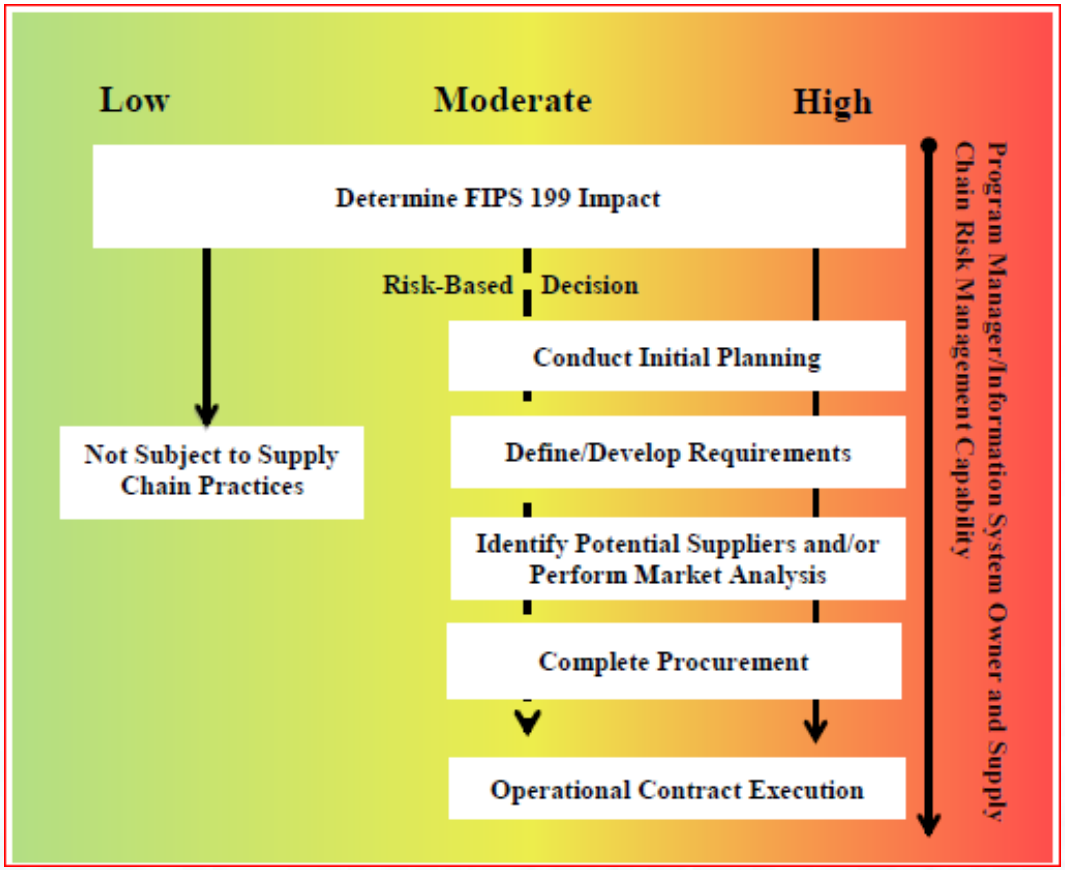
OEM, or Design Activity

Authorized (by OEM) remanufacturer

Authorized Franchise Distributor

Authorized Distributor

Open Market



From NIST.IR.7622 Notional Supply Chain Risk Management Practices for Federal Information Systems, 2012

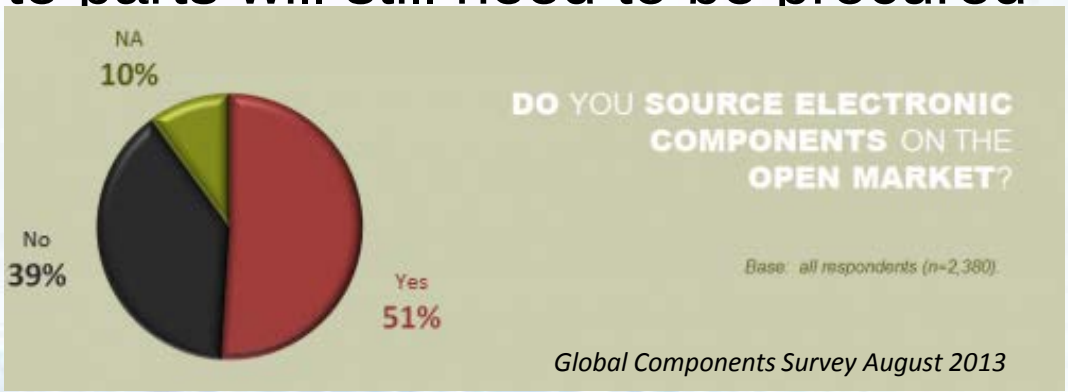
A suite of detection methods must be available

Counterfeit Type		Detection Methods: External VIsual & Phys Dim	XRF Analysis	Mark Perm	Internal Visual	Basic DC Test	Min Func Test 25C	Full Spec Extended Temps	Test & Qual
Non Functioning Devices	No Die	Possible	No	Possible	Yes	Yes	Yes	Yes	Yes
	Wrong Die Re-Marked	Possible	No	Possible	Likely	Yes	Yes	Yes	Yes
	Board Pulls	Possible	No	No	No	Possible	Likely	Yes	Yes
Functioning Devices	Failed Real Parts	No	No	No	No	Possible	Likely	Yes	Yes
	Speed up-marking	Possible	No	Possible	No	No	Possible	Yes	Yes
	Spec up-marking	Possible	No	Possible	No	No	Possible	Yes	Yes
	Temp up-range	Possible	No	Possible	No	No	No	Yes	Yes
	Pb Free Re-marked	Possible	Yes	Possible	No	No	No	No	No
	Lesser part (Knock-off)	Possible	No	Possible	Possible	Possible	Possible	Likely	Yes

Unsure of original source: Integra, BAE-H Livingston, IDA

Obsolete and COTS parts

- Parts currently in inventory, but not in the queue (purchased) for a current DoD program are not exempt from traceability and authentication requirement
- The realities of dealing with COTS OEMs
  - Frequently need OCM to verify the IP on the part
- COTS parts can be listed on GSA schedules without conforming to these requirements
- Vast numbers of obsolete parts will still need to be procured on the open market



Where have your parts been?

Example 1: The practice of returning excess inventory for supplier credit will change:

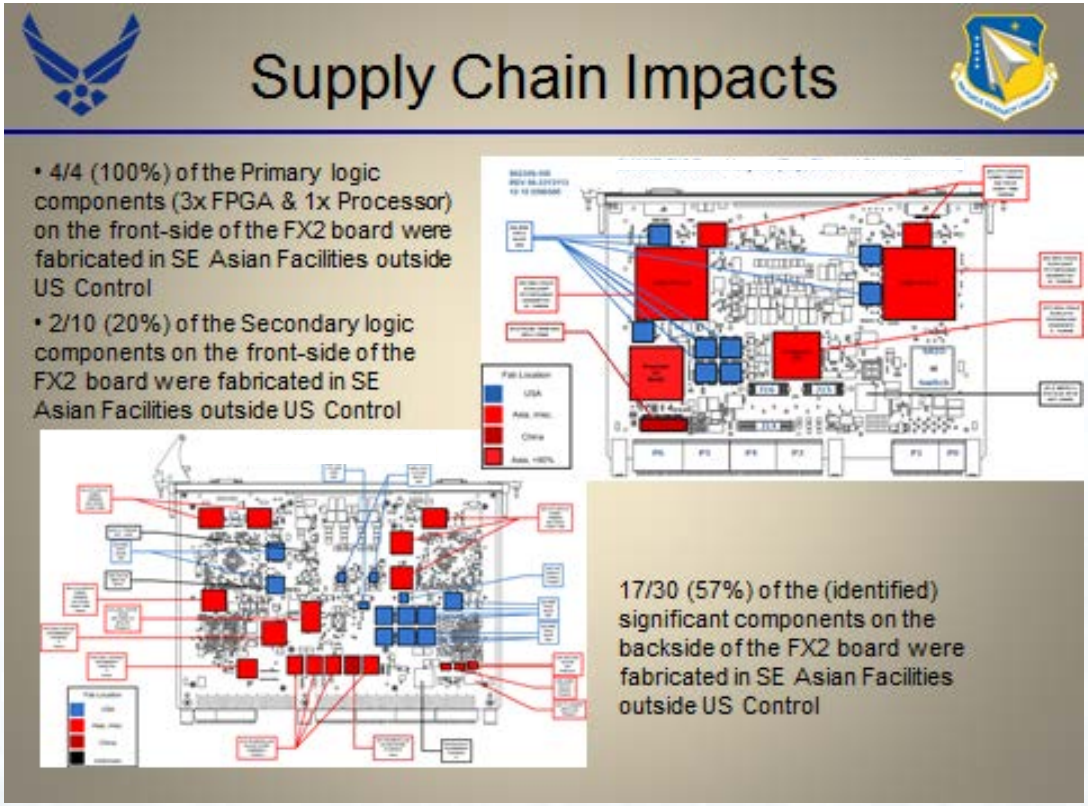
- Last year a customer returned parts for credit to a distributor who resold them to a defense customer. The original parts were good, the returns were fakes.
- Expect to be charged for testing of returned parts.

Example 2: Here's a real world 100% COTS FPGA processor board

Parts purchased from catalogs by division in Canada

Parts kitted and shipped to the US for assembly and test

Traceability for parts is lost, but the board is tested and functioning when delivered.



Comments

How will this affect your company?

How is your company reacting now?

wyle

References

- Contract Clause Language
  - http://www.acq.osd.mil/dpap/dars/dfars/html/current/252244.htm#252.244-7001
- Link to Federal Register Analysis of Public Comments
  - https://www.federalregister.gov/articles/2014/05/06/2014-10326/defense-federal-acquisition-regulation-supplement-detection-and-avoidance-of-counterfeit-electronic#h-31
- Source for supply chain counterfeit risk calculator(s)
  - http://inemi.org/
  - G19_SAE
- Penton's Design Engineering & Sourcing Group Survey
  - http://globalpurchasing.com/counterfeit/counterfeit-electronic-components-survey

The United States Senate Armed Services Committee's ("SASC") investigation announced eight key conclusions:

- **Conclusion 1:** China is the dominant source country for counterfeit electronics parts that are infiltrating the defense supply chain.
- **Conclusion 2:** The Chinese government has failed to take steps to stop counterfeiting operations that are carried out openly in that country.
- **Conclusion 3:** The Department of Defense lacks knowledge of the scope and impact of counterfeit parts on critical defense systems.
- **Conclusion 4:** The use of counterfeit electronic parts in defense systems can compromise performance and reliability, risk national security, and endanger the safety of military personnel.
- **Conclusion 5:** Permitting contractors to recover costs incurred as a result of their own failure to detect counterfeit electronic parts does not encourage the adoption of aggressive counterfeit avoidance and detection programs.
- **Conclusion 6:** The defense industry's reliance on unvetted independent distributors to supply electronics parts for critical military applications results in unacceptable risks to national security and the safety of U.S. military personnel.
- **Conclusion 7:** Weaknesses in the testing regime for electronic parts create vulnerabilities that are exploited by counterfeits.
- **Conclusion 8:** The defense industry routinely failed to report cases of suspect counterfeit parts, putting the integrity of the defense supply chain at risk.