

**June 28, 2016**

## **Counterfeit Electronic Parts & Electronic Supply Chain Symposium**

College Park, MD

# ***JEDEC's New JESD243: Is It an Industry Standard for Counterfeit Electronic Parts – or Something Less?***

**Robert S. Metzger**

Rogers Joseph O'Donnell, P.C.

875 15<sup>th</sup> Street, N.W., Ste 725 | Washington, D.C. 20005

Phone: (202) 777-8951 | Cell: (213) 880-4224

[rmetzger@rjo.com](mailto:rmetzger@rjo.com) | [www.rjo.com](http://www.rjo.com)

**Mark Northrup**

VP of Advanced Technical Operations & Strategy,

IEC Electronics

Phone: (315) 332-4283 | Cell: (315) 573-2837

[MNorthrup@iec-electronics.com](mailto:MNorthrup@iec-electronics.com) | [www.iec-electronics.com](http://www.iec-electronics.com)

*Thanks to Oliya Zamaray of RJO for her assistance*

# Introduction

**Increasingly, both government and industry look to industry standards and best practices to assist in supply chain security.**



- **From the government standpoint:**
  - Standards and practices can assist the Government (DoD) in its efforts to reduce the risk of counterfeit electronic parts
  - Standards and practices inform contractors on how to identify and mitigate supply chain risk
  - Emerging supply chain threats (e.g., IoT) call for new standards
- **From industry's standpoint:**
  - Standards act as “reference points” to assure compliance with new government supply chain initiatives
  - Well-developed standards and practices can advance the art and practice of dealing with real-world supply chain events
  - Risk-based assessment and response are promoted

# Introduction

However, not all standards are both constructive and effective. Standards that ratify existing industry behavior may fall short of need, as would standards that offer only general principles but not sufficient detail. Standards that reflect a “consensus” among divided stakeholders may lack focus and suffer from diluted benefit.



Today, we will examine:

- Why it is important for government and industry to utilize standards and best practices to deal with new supply chain threats
- Tensions between cost and value, specificity and practicality, implications for competition and the importance of assessment and accreditation
- How standards and best practices figure today into government regulations that affect the supply chain – and what can be expected
- Distinguishing between valuable standards and those that disappoint

# Background

- **May 6, 2014 – DOD issued a final rule on Detection and Avoidance of Counterfeit Electronic Parts (79 Fed. Reg. 26092).**
  - DOD expressed its agreement with use of “industry consensus standards . . . for the development and implementation of internal counterfeit parts detection and avoidance systems” (79 Fed. Reg. at 26102).
  - Required larger contractors to employ counterfeit avoidance systems that satisfy 12 specified criteria. DFARS 252.246-7007.
  - Four of the 12 criteria made explicit reference to industry standards:
    - inspection and testing (#2)
    - traceability (#4)
    - systems to detect and avoid (#8) and
    - keeping informed (#10)

# Background

- **Sept. 21, 2015 – DOD issued a proposed rule to modify the existing DFARS (80 Fed. Reg. 56939), assigning even more importance to industry standards.**
  - If a DOD contractor uses “DoD-adopted counterfeit prevention industry standards,” it will be able to identify “trustworthy” suppliers who are other than original sources. Proposed DFARS 246.870-1, 80 Fed. Reg. at 56843.
  - Where it is necessary to use a part sourced from a “non-trusted supplier,” the proposed DFARS would hold the contractor responsible to inspect, test and authenticate “in accordance with existing applicable industry standards.” Proposed DFARS 252.246-70XX(d)(2), 80 Fed. Reg. at 56944.

# Background

- **JEDEC**
  - Now, the JEDEC Solid State Technology Association
  - Has nearly 300 members in the microelectronics industry
  - Represents itself as “the global leader in developing open standards for the microelectronics industry”
- **“Counterfeit Electronic Parts: Non-Proliferation for Manufacturers” (JESD243)**
  - March 24, 2016 – JEDEC published JESD243, directed at all manufacturers of electronic parts
  - Sought to define “standard requirements for developing both a mitigation policy and a product return policy, including return verification and a prohibition on the restocking of confirmed counterfeit” parts.

# JEDEC's New JESD243

## Critique – Overview

- Most useful to device manufacturers; accommodates existing and individual business practices that maximizes manufacturers' market opportunity
- Less useful for those who build and support systems with electronic parts
- Contemplates purchase only from the original device maker, its authorized distributors, or approved aftermarket manufacturers
- Does not address threat from counterfeit electronics in sustainment of systems where the needed part is no longer in production or available from original (or “trusted”) sources
- Calls upon device manufacturers to adopt policies but fails to provide substance and is vague on details

Compared with other industry standards, JESD243 does not express and elaborate upon norms or advance “best practices” or technical methods.

# Scope

## JESD243:

- **Scope (No. 1)** - purports to identify “the best commercial practices for mitigating and/or avoiding counterfeit products by all manufacturers of electronic parts.”
- **Length:** 8 pages

## Critique:

- JESD243 promises more than delivers.
- While “requirements” include a documented counterfeit mitigation policy, it provides no details on what is satisfactory.
- JESD243 is a “policy of policies.” It does not call for specific or consistent measures.

## Other Standards:

- SAE has multiple standards released or in process to address counterfeit prevention:
  - AS 5553 (OEMs/Users of Electronics)
  - AS 6081 (Independent Distributors/Brokers of Electronics)
  - AS 6486 (Authorized Distributors of Electronics)
  - AS 6171 (Test Methods Standard (in ballot))
- Other useful standards include OTTP-S v. 1.1 (The Open Group)

# Reporting

## JESD243:

- **Reporting (No. 4.1)** – calls for policies for disposition and reporting of parts determined to be counterfeit.
- **Disposition of returns deemed suspect or counterfeit (No. 4.3.3.d)** – Acknowledges GIDEP (the Government Industry Data Exchange Program)

## Critique:

- Unclear who in the supply chain reports a counterfeit (e.g., supplier, customer, independent third party, or certified laboratory).
- States it is up to the manufacturer to determine whether it is “appropriate” to notify GIDEP.
- No reference to other reporting bodies or obligations.

## Other Standards:

- **AS 5553A** – reporting addressed at §4.1.9 and App. G. Requires Organization to report occurrences of suspect/confirmed counterfeits to the “Authority Having Jurisdiction.” Provides list of reporting contact sources.
- **AS 6081** – reporting addressed at § 4.2.9 and Appx. D.
- **DLA QSLD** – §4.3.2 requires distributor to report product discrepancies/corrective action to DLA-VQ.
- Valuable commercial sources of information on product nonconformity, such as ERAI ([www.era.com](http://www.era.com))

Reporting is required by § 818 and by the DFARS (System Criteria 6) but the volume of reports submitted to GIDEP suggests improvements are needed to resolve questions as to reporting responsibility. Standards could help.

# CD&A Plan Requirements

## JESD243:

- **Control Plan (No. 4.2)** – requires manufacturers to develop and implement a “counterfeit parts control plan”

## Critique:

- Required “minimum processes” are largely protective of OEMs as exclusive sources of supply.
- Few details are provided beyond high-level requirements (i.e., maintain lists of authorized distributors/suppliers, use approved distribution agreement, restrictions on sources of parts and raw materials, delivery documentation).

## Other Standards:

- **AS 5553A** - §4.1 (Fraudulent / Counterfeit EEE Parts Control Plan) requires documentation of processes used for risk mitigation, disposition, and reporting. Plan must include:
  - 4.1.1 Personnel Training
  - 4.1.2 Parts Availability
  - 4.1.3 Purchasing Process
  - 4.1.4 Purchasing Information
  - 4.1.5 Verification of Purchased/Returned Parts
  - 4.1.6 In-Process Investigation
  - 4.1.7 Failure Analysis
  - 4.1.8 Material Control
  - 4.1.9 Reporting
  - 4.1.10 Post Delivery Support
- **AS 6081** – similarly detailed guidance

# Authorized Distributors

## JESD243:

- Strongly favors use of authorized distributors

## Critique:

- Contains virtually no minimum requirements for selecting and maintaining such distributors.

## Other Standards:

- SAE AS6081 (“Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors”) discusses in detail appropriate handling, material and inventory control, quality processes, and detection criteria for counterfeit parts, traceability, and the like.

# Minimum Process

## JESD243:

- Authorized Distributors List (No. 4.2.1)
- Distribution Agreement (No. 4.2.2)
- Approved Suppliers Listing (No. 4.2.3)
- Purchase Restriction (No. 4.2.4)
- Commercial, industrial and automotive parts (No. 4.2.5)
- Military Parts (No. 4.2.6)
- Organization's CoC (No. 4.2.7)
- Retention of Records (No. 4.2.8)
- Control of Nonconforming Product and Excess Materials (No. 4.2.9).

## Critique:

- “Minimum processes” are stated generally; justify existing practices rather than improve measures device manufacturers employ to control supply chain.
- Helpful to the “supply” side of the supply chain, but is less so to the “demand” side because it offers little granularity to assure device purchasers.

## Other Standards:

- **AS 5553A** and **AS 6081** provide detailed guidance on the minimum processes necessary for risk mitigation, disposition, and reporting.
- Designed to provide uniform requirements, practices, and methods to mitigate the risks of *receiving* and installing fraudulent/counterfeit parts.
- Helpful to device manufacturers and device purchasers alike.

# Traceability

## JESD243:

- **Supply Chain Traceability (No. 3)** – defined as documented evidence of a part's supply chain history.
- **Return Verification (No. 4.3.2)** – before a manufacturer restocks parts returned to it, it must validate the parts against the traceability records

## Critique:

- Beyond definition, no general obligation on device manufacturers to ensure products, once delivered, are traceable either through accompanying documentation or through technical means to verify authenticity.
- Does not serve needs of system purchasers, operators, or maintenance providers

## Other Standards:

- **AS 5553A** – must document all supply chain intermediaries and significant handling transactions (i.e., from OCM to distributor; from excess inventory to broker to distributor). Appx. C offers guidance on Supply Chain Traceability. Verification of Purchased / Returned Parts addressed at §4.1.5.
- **AS 9120** –§7.5.3 (Identification and Traceability) details the necessary processes.
- **DLA QSLD** requires documented trail through all Distributors, intermediate possessors, to the specified Approved Manufacturer

# “Permissive” Requirements

## JESD243:

- **Disposition of returns deemed suspect or counterfeit (No. 4.3.3)** - confirmed counterfeits shall not be returned to the customer, but the manufacturer “may” decide to retain them or to turn over to law enforcement.

## Critique:

- JESD243 is “permissive” in important areas.
- If a part is confirmed counterfeit, no absolute instruction in No. 4.3.3 (to the supplier, customer, independent third party, entity on the spot) as to disposition, whether it be to quarantine or destroy.
- No obligation to preserve evidence, or inform potentially at-risk users.
- No stated “best practice” for forensic investigation to determine the source of the counterfeit or to take measures to act against such sources.

## Other Standards:

- **AS 5553A** requires at §4.1.8 methods that control confirmed counterfeit parts to “preclude their use or reentry into the supply chain” by (i) physically identifying and (ii) segregating the parts from acceptable parts and (iii) placing in quarantine.
- **AS 5553A** requires at §4.1.9 methods that assure “all occurrences” of suspect or confirmed counterfeits are reported to internal organizations, customers, government reporting organizations, etc.
- **AS 9120** requires at §8.5.3 preventive action to “eliminate the causes of potential nonconformities” to prevent their occurrence.

# Return Verification

## JESD243:

- **Return Verification (No. 4.3.2)** - If parts are returned to the manufacturing organization, the manufacturing organization is obliged to perform “return verification” before return of parts to stock or resale.

## Critique:

- Does not specify how and with what methods to perform the “return verification.”
- Important question left to the discretion of each manufacturer.

## Other Standards:

- Other standards we have reviewed do not specify the methods manufacturers *must* use to perform “return verification”
- **AS 5553A** includes at Appx. E (Product Assurance) detailed tests a manufacturer *might* use in its efforts to detect counterfeit parts among returned products. Also, Appx. F steps for supplier validation of authenticity.

# Certificates of Conformance

## JESD243:

- **Organization's Certificate of Conformance (No. 4.2.7)** – states that CoC “data content may include” enumerated subjects, such as the name of the manufacturing organization, the part number, date and lot code, etc.

## Critique:

- Leaves it to each manufacturer's “internal procedures” to determine whether and with what content a CoC will be provided.
- Minimum CoC obligations would have served interests of buyers and other downstream supply chain participants.

## Other Standards:

- **AS 5553A** directs at §D.3.3 that a manufacturer's CoC “should include the following”:
  - Manufacturer name and address
  - Manufacturer and/or buyer's full part number and part description
  - Batch identification for the item(s) such as date codes, lot codes, serializations, or other batch identifications.
  - Signature/stamp with title of seller's authorized personnel signing the CoC.
- **AS 6081** similarly requires at §B.1.4 that a manufacturer's CoC “shall, at minimum, include” the information listed above.

# Production Overruns

## JESD243:

- **Control of nonconforming product and excess materials (No. 4.2.9)** – “policy” and “methodology” required to keep production overruns from re-entering the supply chain.

## Critique:

- Does not obligate manufacturers to strictly control production overruns.
- No particulars are provided (as to how, when, what, using which standards, and so forth).

## Other Standards:

- **AS 5553A** requires at §4.1.8 specific methods to “control excess and nonconforming parts to prevent them from entering the supply chain under fraudulent circumstances”
- **AS 5553A** requires at Appx. F (Material Control) control of excess inventory or surplus parts.
- **AS 6081** requires at §4.2.8 control of excess and nonconforming parts to prevent them from entering the supply chain under fraudulent circumstances.

# Verifying Authenticity

## JESD243:

- JESD243 provides little content on this important subject, though technical methods are available for determining the authenticity of electronic parts.

## Critique:

- Does not consider that semiconductor makers use sophisticated (often proprietary) methods to uniquely identify their products.
- Does not facilitate the ability of customers and users to verify authenticity by reference to such methods and unique device signatures.

## Other Standards:

- Many technical means are employed by manufacturers and test specialists, and others are emerging.
- SAE is in the final stages of completing AS 6171, “Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts.”

# Life Cycle Issues

## JESD243:

- JESD243 fails to address “product life cycle,” “components obsolescence,” or “diminishing sources.”

## Critique:

- Obsolescence, non-production, diminishing manufacturing sources and material shortages (DMSMS), increase the risk of counterfeits.
- JESD243 does not assign responsibility to device manufacturers to plan for these conditions or inform stakeholders when such conditions are imminent.
- No duty of cooperation to address technical solutions (emulation, cooperation to facilitate contract manufacture, etc.) to parts shortages.

## Other Standards:

- **AS 5553A** requires at §4.1.2 that written processes maximize availability of authentic, originally designed and/or qualified parts throughout the product’s life cycle, including management of parts obsolescence. Information and guidance on obsolescence management is provided in Appx. A.

# After-market Manufacturers

## JESD243:

- **Authorized aftermarket manufacturer (No. 3)** – a manufacturer that meets one or more stated criteria.

The Proposed DFAR, if adopted, would enable contractors to identify non-OEM suppliers as “trustworthy” using “DoD-adopted counterfeit prevention industry standards and processes, including testing.” 80 Fed. Reg. 56944. JESD243 does not inform or facilitate such qualification.

## Critique:

- Does not establish qualification standards or verification measures.
- Excludes legal “reverse-engineering” without the permission of the rights holder of the original intellectual property (IP).
- Unclear whether an “authorized aftermarket manufacturer” must inform customers that a part it has produced (with authorization) is different from original.

## Other Standards:

- **AS 5553A** explains at §3.4 that an aftermarket manufacturer:
  - *Authorized* by OCM to produce/sell replacement parts (usually due to OCM decision to discontinue production). Allows aftermarket manufacturer to use materials transferred from the OCM, or produced using OCM tooling and IP.
  - Aftermarket production, including reverse-engineering, relies on processes that match OCM’s specifications and satisfy customer needs without violating the OCM’s IP.
  - Parts must be labeled to avoid confusion with parts made by OCM
- **AS 6081** – similar req’s at §3.4.

# Records Retention

## JESD243:

- **Retention of Records (No. 4.2.8)** – manufacturing organization shall “document and maintain records in accordance with their internal quality system standards.” Records are to be suitable in “format, accuracy, and detail to permit analysis by the organizations internal quality personnel and government agencies.”

## Critique:

- Cursory and deferential to company election rather than prescriptive of “best practices” or expected, “standard” methods.
- Does not recognize the interests of customers in the content or availability of retained records.

## Other Standards:

**AS 9120** states at §4.2.4 that records shall include:

- manufacturer, distributor, repair station, test and inspection reports;
- original CoCs (manufacturer, sub-tier distributor), copies of airworthiness certificates;
- non-conformance, concession and corrective action records;
- lot traceability records;
- environmental or shelf life condition records.
- If electronic – system integrity and back-up procedures must be validated.
- Records must not be capable of change by software; must be traceable to the original documentation.
- Maintain for 7 yrs (min).

# Final Comments

- Compliance with industry standards and best practices already is important in regulation and as guidance to supply chain participants
- Industry standards will acquire more importance as regulations evolve and apply to more suppliers
- Counterfeit Avoidance standards should address and mitigate key risks
  - Diminishing sources & obsolescence
  - Continuing demand for parts not available from “trusted” suppliers
  - Qualification of “trustworthy” suppliers (per Proposed DFARS)
  - Assurance through traceability of both “pedigree” and “provenance”
  - Appropriate inspection and test methods to verify parts authenticity
  - Obligation to quarantine and assignment of reporting responsibilities
  - Compliance with the 12 specified criteria of DFARS 252.246-8007
  - *Prospectively – protecting against “taints” and malicious code*

JESD243 can be improved to respond to supply chain needs.

# About the Presenters



Robert S. Metzger  
Rogers Joseph O'Donnell PC  
202-777-8951  
[Rmetzger@rjo.com](mailto:Rmetzger@rjo.com)

Robert S. Metzger heads the Washington, D.C. office of Rogers Joseph O'Donnell, P.C., a boutique law firm that specializes in public procurement matters. He advises leading U.S. and international companies on key public contract compliance challenges and in strategic business pursuits. Bob is recognized for work on supply chain and cyber security. On these subjects, he has published extensively and has made presentations to many government, industry, legal and technical groups, among them ABA (PCL, S&T, SLD), AIA, ASIS, CALCE, CFAM, DoD, DIB SCC, DoJ, DSB, ERAI, Georgetown Law Cyber Institute, IPC, National IPR Center, NCMA, NDIA, SAE, SMTA and SSCA.

Recently named a 2016 "Federal 100" awardee, Federal Computer Week said of Bob: "In 2015, he was at the forefront of the convergence of the supply chain and cybersecurity, and his work continues to influence the strategies of federal entities and companies alike."

Bob is a member of the Defense Science Board Cyber/Supply Chain Task Force. He also is Vice-Chair of the Cyber/Supply Chain Assurance Committee of the IT Alliance for Public Sector (ITAPS), a unit of the Information Technology Industry Council (ITIC), a prominent trade association.

Bob received his B.A. from Middlebury College and his J.D. from Georgetown University Law Center, where he was an Editor of the Georgetown Law Journal. He was a Research Fellow, Center for Science & International Affairs (now "Belfer Center"), Harvard Kennedy School of Government. Bob is a member of the International Institute for Strategic Studies (IISS), London. Academic publications on national security topics include articles in *International Security* and the *Journal of Strategic Studies*.

**This presentation reflects Mr. Metzger's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.**

# About the Presenters



## Mark Northrup

VP of Advanced Technical Operations & Strategy, IEC Electronics

[MNorthrup@iec-electronics.com](mailto:MNorthrup@iec-electronics.com)

Mark Northrup has 30 years of experience in electronics design engineering and manufacturing. He has held technical leadership and management positions with increasing levels of responsibility supporting the transportation, optics, aviation, medical, automotive, telecommunications, energy and industrial markets. He is an expert in materials science, testing and analysis, components, PCBs, PCB assemblies, failure analysis, and components counterfeit risk mitigation. He has led test design engineering and new product development while providing executive level technical direction and business development strategy. At IEC, he concurrently serves as Vice President of Advanced Technical Operations and Strategy in Newark, NY and President of Analysis & Testing Laboratory at IEC (formerly Dynamic Research and Testing Laboratories, an IEC company) in Albuquerque, NM.

As Principal Engineer/Manager at GE Transportation, he standardized and institutionalized technical specifications to improve GE's global supply chain quality for electronics across the aviation, transportation, energy, and healthcare businesses. He was Reliability Manager for Optical Devices at Emcore and Section Manager, Failure Analysis Lab at Motorola Automotive Industrial Electronics Group. After one year at IEC, he spearheaded, directed, and built a start-up 'analysis and test services' company as part of the corporation's core business. He continues to oversee and operate this industry-respected laboratory which offers a wide range of testing services, capabilities, and methods for electronic components, material and product qualification, and counterfeit risk mitigation strategies for high reliability electronics. Through his leadership, the lab is highly certified (IPC, ISO, DLA approved, SAE/AS, NADCAP, ANSI, and MIL-STD). He is actively involved in IPC, SMTA (Empire Chapter President 2015-2016), AIA, iNEMI, ERAI Nadcap, SAE organizations. He has recently become involved with NY Photonics/Rochester Regional Photonics Cluster. He holds a Bachelor Degree in Physics and a MS Degree in Materials Science and Engineering from Rochester Institute of Technology.

**This presentation reflects Mr. Northrup's personal views and should not be attributed to any client of his firm or organization with which he is involved or affiliated.**