JESD243: An Industry Standard for COUNTERFEIT ELECTRONIC PARTS – or Something Less?

Counterfeit avoidance standards need additional detail for addressing and mitigating key risks.

by ROBERT S. METZGER and MARK NORTHRUP

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 US government (Department of Defense) in its efforts to reduce the risk of counterfeit electronic parts. Standards and practices also inform contractors on how to identify and mitigate supply chain risk.

Against this backdrop, emerging supply-chain threats (e.g., parts "tainted" by insertion of malicious code) call for new standards. The massive proliferation of end-point sensors that accompany the IoT presents new attack surfaces and vulnerabilities.

From industry's standpoint, standards act as "reference points" to ensure 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. Standards also can be accompanied by assessment and accreditation measures, helping buyers have confidence in their sources and providing positive competitive distinction for sellers.

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

Herein, we will examine why it is important for government and industry to use 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. Finally, we seek to distinguish between valuable standards and those that disappoint.

Common Standards

Government. On May 6, 2014, the DoD issued a final rule on Detection and Avoidance of Counterfeit Electronic Parts (79 Fed. Reg. 26092). In it, the DoD expresses its agreement with use of "industry consensus standards … for the development and implementation of internal counterfeit parts detection and avoidance systems."[1]

The rule requires larger contractors employ counterfeit avoidance systems that satisfy 12 specified criteria.[2] Four of the 12 criteria make explicit reference to industry standards, including inspection and testing (#2), traceability (#4), systems to detect and avoid (#8) and keeping informed (#10).

On Sept. 21, 2015, the DoD issued a proposed rule to modify the existing Defense Federal Acquisition Regulation Supplement (DFARS) (80 Fed. Reg. 56939), assigning even more importance to industry standards. Under the still-pending rule, if a DoD contractor uses DoD-adopted counterfeit prevention industry standards, it will be able to identify "trustworthy" suppliers that are other than original sources.[3] 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."[4] On Aug. 2, 2016, the DFARS was further revised by Final Rule (81 Fed. Reg. 50635). DFARS 252.246-7008 now establishes the basis for purchase from three different categories (or tiers) of sources, expresses traceability requirements and makes new use of risk-based methods for inspection, test and authentication (IT&A). The second "tier" of allowed supplier, under the revised DFARS, is a "contractor-approved supplier (CAS)," which must use "established counterfeit prevention industry standards and processes (including inspection, testing and authentication) [DFARS 252.2467008(b)(2)(i)]. A third tier, of purchase from "other" sources, also is allowed when a needed part cannot be obtained either from the original source or a "contractor-approved supplier." When resort is made to a third-tier supplier, again the DFARS requires "inspection, testing, and authentication (IT&A), in accordance with existing applicable industry standards" [DFARS 252.2467008(b)(3)(ii)(B)].

Industry. On Mar. 24, 2016, JEDEC published JESD243, "Counterfeit Electronic Parts: Non-Proliferation for Manufacturers," directed at all manufacturers of electronic parts. That document 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.[5]

JESD243 is seen as most useful to device manufacturers, as it accommodates existing and individual business practices that maximize manufacturers' market opportunities. It is less useful for those that build and support systems with electronic parts. The standard contemplates purchase only from the original device maker, its authorized distributors or approved aftermarket manufacturers. It does not address threats from counterfeit electronics in sustainment of systems where the needed part is no longer in production or available from original (or "trusted") sources. In contrast, as revised in August 2016, the DFARS now allows purchase either from "contractor-approved suppliers (CAS)" or "other" sourced, but industry standards must be used for inspection, testing and authentication (IT&A) and to approve a second-tier "contractor-approved supplier (CAS)." JESD243 misses the mark because it does not assist with authentication of parts from either second or third tier suppliers.

Compared with other industry standards, JESD243 does not express and elaborate on norms, advance "best practices" or technical methods. It calls on device manufacturers to adopt policies, but fails to provide substance and is vague on details.

Per its scope, JESD243 purports to identify "the best commercial practices for mitigating and/or avoiding counterfeit products by all manufacturers of electronic parts." To that end, JESD243 promises more than it delivers. While "requirements" include a documented counterfeit mitigation policy, it provides no details on what is satisfactory. Indeed, JESD243 is a "policy of policies." It does not call for specific or consistent measures. Considered in the context of the DFARS, JESD243 does not seem to offer the detail that contractors likely need, and which will benefit DoD, to assure that reliance on standards produces the intended result of authenticity.

Others. SAE has multiple standards released or in process to address counterfeit prevention. These include AS5553[6] (for OEMs/users of electronics), AS6081[7] (independent distributors/brokers of electronics), AS6496[8] (authorized distributors of electronics), and AS6171,[9] the test methods standard, recently authorized for final release. Other useful standards include OTTP-S v. 1.1 (The Open Group), which now has been issued as ISO 20243. This new standard deals with mitigation of both "maliciously tainted" and "counterfeit" products.

Review of Requirements

Disposition and reporting. JESD243 calls for disposition and reporting of parts determined to be counterfeit. In doing so, it acknowledges the Government Industry Data Exchange Program (GIDEP), a government/industry

collaboration for sharing technical information essential during research, design, development, production and operational phases of the lifecycle of systems, facilities and equipment.

JESD243 leaves unclear, however, who in the supply chain reports a counterfeit (e.g., supplier, customer, independent third party, or certified laboratory). It leaves it to the manufacturer to determine whether it is "appropriate" to notify GIDEP. It contains no references to other reporting bodies or obligations. This runs against the grain of the DFARS, as the sixth of the 12 system criteria calls for reporting of counterfeit electronic parts and suspect counterfeit electronic parts to GIDEP.

On Aug. 30, 2016, DoD also revised DFARS regulations that are the "cost principles" governing the allowance of costs when charged to defense cost-reimbursement or flexibly priced contracts (81 Fed. Reg. 59515). This important regulatory development enlarges the "safe harbor" available to contractors should a counterfeit escape occur. In such event, costs to replace a counterfeit, and of rework, can be allowable if three conditions are met. One of those conditions is that the contract provides timely notice to both the contracting officer and GIDEP. (The other conditions are having an operational system to detect and avoid counterfeit electronic parts that has been approved by DoD and that the part was obtained from one of the three tiers of allowed sources.)

Among the other standards, AS5553A covers reporting in section 4.1.9 and Appendix G. AS5553A requires the organization to report occurrences of suspect/confirmed counterfeits to the "authority having jurisdiction." It also provides a list of reporting contact sources.

AS6081 addresses reporting in section 4.2.9 and Appendix D. DLA QSLD section 4.3.2 requires the distributor to report product discrepancies/corrective action to the Defense Logistics Agency Sourcing and Qualifications Division (DLA-VQ). There also are valuable commercial sources of information on product nonconformity, such as ERAI (erai.com).

Reporting is required by AS6081 section 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. Especially with the DFARS revisions, companies should be actively encouraged to make timely reporting, to GIDEP (when eligible), because there could be adverse financial and compliance consequences should a company become aware of a counterfeit or suspect part but fail to report.

CD&A plan requirements. JESD243 requires manufacturers develop and implement a "counterfeit parts control plan" (No. 4.2). The required "minimum processes" are largely protective of OEMs as exclusive sources of supply. It provides few details 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).

AS5553A, section 4.1 (Fraudulent/Counterfeit EEE Parts Control Plan) requires documentation of processes used for risk mitigation, disposition, and reporting. Such plans must detail personnel training, parts availability, purchasing process, purchasing, verification of purchased/returned parts, in-process, failure analysis, material control, reporting, and post-delivery support. AS6081 calls for similarly detailed guidance.

Authorized distributors. JESD243 strongly favors use of authorized distributors. It contains virtually no minimum requirements for selecting and maintaining such distributors, however.

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.

The revised DFARS now endorses use of "contractor-approved suppliers (CAS)," which may be distributors that a purchasing contractor qualifies to supply parts not available for the most trusted tier of suppliers. As noted, the qualification of such suppliers is to be informed by industry standards, as is the selection and conduct of inspection, testing, and authentication (IT&A). JESD243 does not help to inform or clarify what measures should be taken.

Minimum process. In JESD243, "minimum processes" are stated generally and justify existing practices, rather than improving measures device manufacturers employ to control their supply chains. This is helpful to the "supply" side of the supply chain, but is less so to the "demand" side because it offers little granularity to ensure device purchasers.

AS5553A and AS6081 provide detailed guidance on the minimum processes necessary for risk mitigation, disposition and reporting. They are designed to provide uniform requirements, practices and methods to mitigate the risks of *receiving* and installing fraudulent/counterfeit parts. This is seen as helpful to device manufacturers and device purchasers.

Traceability. Under JESD243, supply-chain traceability (No. 3) is defined as documented evidence of a part's supply-chain history. The standard's section on Return Verification (No. 4.3.2) states that before a manufacturer restocks parts returned to it, it must validate the parts against the traceability records.

Beyond the definitions, the standard establishes no general obligation on device manufacturers to ensure products, once delivered, are traceable either through accompanying documentation or through technical means to verify authenticity. Nor does it serve the needs of system purchasers, operators, or maintenance providers.

These limitations are especially unfortunate in light of the August revisions to the counterfeit parts DFARS. The least favored category of sources – the "third tier" – are "other sources" when parts cannot be obtained from the two higher and more trusted tiers. A part can fall into this third tier if a company cannot "confirm" that an electronic part "is new or previously unused and that it has not been comingled in supplier new production or stock with used, refurbished, reclaimed or returned parts." DFARS 252.2467008(b)(3)(i)(B). JESD243 does not impose a positive obligation on a manufacturer to create or maintain documentation sufficient to satisfy the DFARS concern with comingled parts.

Users of AS5553A must document all supply chain intermediaries and significant handling transactions (i.e., from OCM to distributor; from excess inventory to broker to distributor). Appendix C offers guidance on supply chain traceability, while verification of purchased/returned parts is addressed in section 4.1.5. AS9120. Section 7.5.3 (Identification and Traceability) details the necessary processes. DLA QSLD requires a

documented trail through all distributors and intermediate possessors to the specified, approved manufacturer.

The revised DFARS contains specific traceability requirements at 252.2467008(c), which apply if a contractor is not the original manufacturer, or an authorized supplier for, an electronic part. Where a contractor cannot establish traceability from the original manufacturer, it must "be responsible for inspection, testing, and authentication (IT&A), in accordance with existing applicable industry standards." JESD243's limited treatment of traceability makes it more likely that DoD suppliers will experience parts with less documentation that DoD desires and that additional inspection, testing and authentication will be required because of the absence of sufficient traceability documentation.

'Permissive' requirements. For disposition of returns deemed suspect or counterfeit, JESD243 states confirmed counterfeits shall not be returned to the customer, but the manufacturer "may" decide to retain them or to turn them over to law enforcement. This is "permissive" in important areas. If a part is a confirmed counterfeit, JESD243 contains no absolute instruction (to the supplier, customer, independent third party, or entity on the spot) as to disposition, whether it be to quarantine or destroy. There is no obligation to preserve evidence, or inform potentially at-risk users. Nor is there a stated "best practice" for forensic investigation to determine the source of the counterfeit or to take measures to act against such sources.

JESD243 again is less than what is needed to facilitate compliance with the revised DFARS. The sixth of the 12 system criteria requires both reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts. It does not permit companies with systems to detect and avoid counterfeit parts to return an electronic part, either to the seller or to the supply chain. "until such time that the parts are determined to be authentic" [DFARS 252.2467007(b)].

In contrast, AS5553A section 4.1.8 requires 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. AS5553A section 4.1.9 requires methods that ensure "all occurrences" of suspect or confirmed counterfeits are reported to internal organizations, customers, government reporting organizations, etc. And AS9120 mandates preventive action to "eliminate the causes of potential nonconformities" to prevent their occurrence (section 8.5.3).

Return verification. JESD243 Return Verification (No. 4.3.2) states that 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. It does not specify how and with what methods to perform the "return verification." This important question is left to the discretion of each manufacturer.

Other standards we have reviewed do not specify the methods manufacturers *must* use to perform "return verification."

AS5553A Appendix E (Product Assurance) includes detailed tests a manufacturer *might* use in its efforts to detect counterfeit parts among returned products. Also, Appendix F steps for supplier validation of authenticity.

Certificates of conformance. Under JESD243 (No. 4.2.7), an organization's Certificate of Conformance "data content may include" enumerated subjects, such as the name of the manufacturing organization, the part number, date and lot code, etc. The standard leaves it to each manufacturer's "internal procedures" to determine whether and with what content a CoC will be provided. The inclusion of minimum CoC obligations would have served interests of buyers and other downstream supply-chain participants.

AS5553A directs that a manufacturer's CoC "should include" 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; and signature/stamp with title of seller's authorized personnel signing the CoC (section D.3.3). AS6081 similarly requires in section B.1.4 that a manufacturer's CoC "shall, at minimum, include" the information listed above.

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

AS5553A section 4.1.8 requires specific methods to "control excess and nonconforming parts to prevent them from entering the supply chain under fraudulent circumstances." Appendix F (Material Control) of AS5553A requires control of excess inventory or surplus parts. AS6081 section 4.2.8 requires control of excess and nonconforming parts to prevent them from entering the supply chain under fraudulent circumstances.

Under JESD243 No. 4.2.9, "Control of Nonconforming Product and Excess Materials," "policy" and "methodology" are required to keep production overruns from reentering the supply chain.

Verifying authenticity. JESD243 provides little content on this important subject, though technical methods are available for determining the authenticity of electronic parts. It does not consider that semiconductor makers use sophisticated (often proprietary) methods to uniquely identify their products. Nor does it facilitate the ability of customers and users to verify authenticity by reference to such methods and unique device signatures.

Other standards recognize many technical means are employed by manufacturers and test specialists, and others are emerging. SAE's newly released AS6171, "Test Methods Standard: General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts," addresses this subject in detail.

Lifecycle issues. JESD243 fails to address "product lifecycle," "components obsolescence," or "diminishing sources." It is felt obsolescence, non-production, diminishing manufacturing sources and material shortages (DMSMS) increase the risk of counterfeits. JESD243, however, does not assign responsibility to device manufacturers to plan for these conditions or inform stakeholders when such conditions are imminent. There is no duty of cooperation to address technical solutions (emulation, cooperation to facilitate contract manufacture, etc.) to parts shortages.

AS5553A requires at section 4.1.2 that written processes maximize availability of authentic, originally designed and/or qualified parts throughout the product's lifecycle, including management of parts obsolescence. Information and guidance on obsolescence management is provided in Appendix A.

After-market manufacturers. Per JESD243 No. 3, an authorized aftermarket manufacturer is a manufacturer that meets one or more stated criteria. It does not establish qualification standards or verification measures for this group. However, it excludes legal "reverse-engineering" without the permission of the rights holder of the original intellectual property (IP). Left unclear is whether an "authorized aftermarket manufacturer" must inform customers that a part it has produced (with authorization) is different from the original.

AS5553A explains in section 3.4 that an aftermarket manufacturer is *authorized* by the OCM to produce or sell replacement parts (usually due to an OCM decision to discontinue production). It permits the 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. Finally, parts must be labeled to avoid confusion with parts made by the OCM.

AS6081 section 3.4 establishes similar requirements. The proposed DFAR (80 Fed. Reg. 56944), if adopted, would enable contractors to identify non-OEM suppliers as "trustworthy," using "DoD-adopted counterfeit prevention industry standards and processes, including testing." JESD243 does not inform or facilitate such qualification.

Records retention. JESD243 (No. 4.2.8) states 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 organization's internal quality personnel and government agencies." This statement is cursory and deferential to company election, rather than prescriptive of "best practices" or expected "standard" methods. Further, it does not recognize the interests of customers in the content or availability of retained records. It may prove insufficient to satisfy the traceability sought by the DFARS.

AS9120 (section 4.2.4) states records shall include manufacturer, distributor, repair station, test and inspection reports; original CoCs (manufacturer, sub-tier distributor), copies of airworthiness certificates; nonconformance, concession and corrective action records; lot traceability records; and environmental or shelf-life condition records. If the latter is electronic, system integrity and backup procedures must be validated. Records must not be capable of change by software, and must be traceable to the original documentation. Records must be maintained for a minimum of seven years.

Final Comments

Compliance with industry standards and best practices already is important in regulation and as guidance to supply-chain participants. With the DFARS revisions in August 2016, industry

standards have taken on even more importance. Counterfeit avoidance standards should address and mitigate key risks, including diminishing sources and 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 252.246-7008; and prospectively protecting against "taints" and malicious code. JESD243 is limited in response to these supply chain needs by not addressing the following issues:

- OCM product discontinuance and DMSMS.
- Provenance or authenticity outside of the authorized chain of custody.
- How customers address risk of counterfeits when parts are not procured through the authorized chain of custody.
- Requiring part manufacturers to identify counterfeit products for OEMs when procured outside of the authorized chain of custody.
- Reporting of counterfeits to appropriate authority and GIDEP.
- Verification of authentic embedded firmware or software.

REFERENCES

1. 79 Fed. Reg. at 26102.
2. DFARS 252.246-7007.
3. Proposed DFARS 246.870-1, 80 Fed. Reg. at 56843.
4. Proposed DFARS 252.246-70XX(d)(2), 80 Fed. Reg. at 56944.
5. JEDEC, JESD243: "Counterfeit Electronic Parts: Non-Proliferation for Manufacturers," March 2016.
6. SAE Intl., AS5553, "Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition," April 2009.
7. SAE Intl., AS6081, "Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors Counterfeit Electronic Parts; Avoidance Protocol, Distributors," November 2012.
8. SAE Intl., AS6496, "Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation and Disposition – Authorized/Franchised Distribution," August 2014.
9. SAE Intl., AS6171, Test Methods Standard: General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts, publication pending.

ACKNOWLEDGMENTS

Thanks to Oliya Zamaray of RJO for her assistance.

Ed.: The content of this article was first presented at the Counterfeit Electronic Parts & Electronic Supply Chain Symposium in June 2016 and is presented here with permission of the authors.

ROBERT S. METZGER heads the Washington, DC, office of Rogers Joseph O'Donnell, P.C. (rjo.com), a boutique law firm that specializes in public procurement matters; rmetzger@rjo.com. **MARK NORTHRUP** is vice president of Advanced Technical Operations & Strategy, IEC Electronics (iec-electronics.com); mnorthrup@iec-electronics.com.