Compliance Programs for Counterfeit Parts Avoidance and Detection

Henry Livingston, BAE Systems Electronic Systems

INTRODUCTION

Counterfeit parts avoidance and detection has emerged as an area of business and legal risk that aerospace and defense (A&D) contractors should incorporate into compliance programs. Section 818 of the National Defense Authorization Act for Fiscal Year 2012[1] requires the Secretary of Defense to *"implement a program to enhance contractor detection and avoidance of counterfeit electronic parts"*. The implementation of this program must include *"processes for the review and approval of contractor systems for the detection and avoidance of counterfeit electronic parts and suspect counterfeit electronic parts"*. Furthermore, DoD's processes for the review and approval of contractor systems are to be similar to those established for *"contractor business systems"* under Section 893 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011. Though these new counterfeit parts avoidance and detection requirements were developed with DoD in mind, both DoD and foreign defense customers (whether Foreign Military Sale or direct commercial) will benefit[2] as US defense suppliers improve their supply chain security.

A&D contractors should established a rule-based compliance program for counterfeit parts avoidance and detection that mitigates risk to the business enterprise and aligns with DoD's expectations described within NDAA 2012 § 818. Though new DoD instructions, implementation guidance and regulations have not been released, Industry and US Government subject matter experts generally agree that the following central tenets should drive effective counterfeit part avoidance and detection practices[3]:

1. Apply supplier preferences for electronic components purchased from original manufacturers or their authorized distributors,
2. Perform due diligence to avoid counterfeits when purchases from sources of supply other than the original component manufacturer and its authorized distribution chain are necessary, and
3. Notify Government and industry of suspect counterfeits when they are encountered.

The following are thoughts for A&D contractors to consider while establishing and implementing a compliance program for counterfeit parts avoidance and detection.

NDAA 2012 § 818(E) – IMPROVEMENT OF CONTRACTOR SYSTEMS FOR DETECTION AND AVOIDANCE OF COUNTERFEIT ELECTRONIC PARTS

Section 818(e) lists several elements that should be addressed within contractor policies and procedures. Though some have yet to be clearly defined, other subsections of NDAA 2012 § 818 provide insight into many of these elements and can help guide compliance program development:

> (i) the training of personnel
>
> (ii) the inspection and testing of electronic parts
>
> (iii) processes to abolish counterfeit parts proliferation
>
> (iv) mechanisms to enable traceability of parts
>
> (v) use of trusted suppliers
>
> (vi) the reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts
>
> (vii) methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit
>
> (viii) the design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts
>
> (ix) the flow down of counterfeit avoidance and detection requirements to subcontractors

DoD has been evaluating contractor counterfeit detection and avoidance systems based on requirements of NDAA 2012 § 818 and key industry standards such as SAE Aerospace Standard AS5553[4]. These evaluations cover purchasing and subcontract management, receiving & inspection, control of nonconforming material, and reporting. Contactors engaged in this assessment activity will gain first hand insight as DoD devises parameters for formal review and approval of contractor systems in this area.

"OVERARCHING DOD COUNTERFEIT PREVENTION GUIDANCE"

According to DoD representatives, the 16 March 2012 DoD memorandum on "*Overarching DoD Counterfeit Prevention Guidance*"[5] describes much of what new regulations will require. This memorandum directs specific actions directed to DoD Departments to "prevent, detect, remediate, and investigate counterfeiting in the DoD supply chain". Here are specific areas appearing within this memorandum that provide insight into areas contractors might consider addressing within compliance programs:

Scope – Though the scope of NDAA 2012 § 818 is specific to "electronic parts", this guidance memo states that particular focus will be expected for "mission critical components", "critical safety items", "electronic parts", and "loadbearing mechanical parts".

Definitions – A definition for "counterfeit materiel" is provided which may appear in forthcoming regulations. A "used item represented as a new item" is highlighted as being potentially subject to "fraudulent representation procedures". Though it does not offer a definition for the term "trusted supplier" [ref NDAA 2012 § 818(c)(3)], the guidance memo describes a clear preference for materiel acquired from the "original equipment manufacturer, original component manufacturer, or an authorized distributor".

Risk mitigation – In the case of "mission-critical components", DoD program managers are expected to implement a risk-based approach described in the *"Program Protection Plan Outline and Guidance"*[6], which includes the requirement to evaluate counterfeit risk and implement countermeasures. For "other than mission-critical components" where a counterfeit risk warrants action, the program risk management plan or systems engineering plan must document risk mitigation for the item. The contractor's compliance program should include provisions for counterfeit risk mitigation that (1) emphasize purchases from the original manufacturers or authorized distributors, and (2) apply "inspection, testing and authentication" [ref NDAA 2012 § 818(c)(3)], when parts are purchased from other than original manufacturers or authorized distributors.

Industry standards – Department-level reviews will identify "appropriate industry standards" for use in contracting requirements. Contractors will likely be expected to apply these standards to suppliers below the prime contract. Further discussion on standards gaps and maturity of standards is appears below.

Notification of certain purchases – Contractors can expect a requirement to notify DoD of purchases of "critical items" from other than original manufacturers or authorized distributors, whether or not a known defect exists or a failure is attributed to the specific item. According to the guidance memo, this requirement is expected to apply to suppliers below the prime contract.

Testing and verification requirements – Contractors can expect testing and verification requirements for items identified as "having high risk for counterfeit potential" (see "definitions" and "risk mitigation") and are acquired from suppliers other than "an original equipment manufacturer, original component manufacturer, or authorized distributor". According to the guidance memo, this requirement is also expected to apply to suppliers below the prime contract.

Reports of suspected or confirmed counterfeit items – Contractors and subcontractors will be expected to report "suspected or confirmed counterfeit items" via the Government-Industry Data Exchange Program (GIDEP)[7], which will serve as the DoD central reporting repository.

Notification of Potential Safety Issues – The guidance memo reaffirms DFARS 252.246-7003[8] which requires a contractor to notify the Government within 72 hours after discovery of "credible information" concerning "nonconformances and deficiencies" for "critical safety items".

Investigation of "suspected counterfeit incidents" – DoD programs will be expected to investigate incidents "confirmed as counterfeit" and report them to "the appropriate criminal authorities". In the case of "suspect counterfeits", the parts should be held until resolution of the potential nonconformance is complete. Parts that are confirmed to be counterfeit should not be returned to the supplier prior to criminal authorities' release for disposition.

Personnel training – DoD is expected to develop and provide training to DoD personnel to address counterfeit avoidance and detection. DoD will likely expect a contractor to training its personnel in conjunction with its compliance program for counterfeit parts avoidance and detection.

INDUSTRY STANDARDS

The DoD memorandum on "*Overarching DoD Counterfeit Prevention Guidance"*, describes how DoD will depend on the use of industry standards for anti-counterfeiting and apply those standards in contracting requirements. A&D contractors should, therefore, incorporate the implementation of key anti-counterfeiting standards and supporting documents within their compliance programs. The document which is generally accepted as the central standard describing how contractors should approach counterfeit parts avoidance and detection is SAE Aerospace Standard AS5553. Newer SAE standards have been developed and others are in process to support the implementation of AS5553 and to cover counterfeit parts avoidance and detection practices to be applied by lower level suppliers (e.g. electronic component distributors).

It is important for DoD personnel and contractors to recognize that while much has been accomplished in recent years toward developing standards for counterfeit parts avoidance and detection, significant gaps remain. The presence of requirements in Quality Management System (QMS) standards and associated certification programs would drive implementation of a robust counterfeit avoidance program throughout the supply chain and foster alignment with new DoD requirements directed to upper tier contractors. Organizations involved in maintaining key US and international QMS standards, however, have yet to embed these requirements into QMS standards and supplier certification programs. With regard to lower level standards developed specifically for counterfeit prevention, a standards gap analysis[9] prepared by the author revels that significant coverage exists for electronic parts, but very limited coverage exists for other parts and materials. Furthermore, standards committees that developed the existing standards for electronic parts are pursuing changes to newly released standards in order to address unresolved issues. In the interim, DoD and contractors will need to bridge implementation gaps by establishing subject matter expertise to select and specify counterfeit prevention practices and to monitor the execution of these practices throughout the supply chain.

CLOSING REMARKS

As A&D companies establish and implement compliance programs for counterfeit parts avoidance and detection, it is important to recognize that a number of implementation issues and standards gaps will take time for DoD and industry to address and resolve. A&D companies, therefore, must be prepared to adjust compliance programs for counterfeit parts avoidance and detection as regulations are developed, industry standards mature, implementation approaches evolve.

Henry Livingston is an Engineering Fellow and Technical Director at BAE Systems Electronic Systems. Henry is BAE Systems Electronic Systems subject matter expert in the Component Engineering field. Henry has published papers on component reliability assessment methods, obsolescence management, semiconductor industry trends and counterfeit electronic components. Henry Livingston was recognized at the DMSMS and Standardization 2009 Conference for his leadership role in the detection, mitigation and reporting of counterfeit parts with the government and industry. Henry is a member of the SAE International G-19 Counterfeit Electronic Parts Committee and major contributor to SAE AS5553; the Industry Advisory Group to the Government-Industry Data Exchange Program; and the IEEE.

REFERENCES

[1] H.R.1540 National Defense Authorization Act For Fiscal Year 2012, Public Law No. 112-081, Section 818. Detection and Avoidance of Counterfeit Electronic Parts.

[2] "New regulation to hit price but not demand for US military sales to India – analysis", Policy and Regulatory Report (PaRR), 13 February 2013.

[3] Livingston, H., "Securing the DOD Supply Chain from the Risks of Counterfeit Electronic Components", October 2010.

[4] SAE International Aerospace Specification AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition

[5] "Overarching DoD Counterfeit Prevention Guidance", Hon. Frank Kendall, Acting Undersecretary of Defense for AT&L (March 16, 2012)

[6] "Protection Plan (PPP) Outline & Guidance", July 2011, Version 1.0

[7] Government-Industry Data Exchange Program (GIDEP)

[8] DFARS 252.246-7003, Notification of Potential Safety Issues

[9] "Counterfeit Prevention, Detection and Avoidance Standards Gap Analysis for Hardware Products", Prepared by Henry Livingston, February 2013