Securing the DOD Supply Chain from the Risks of Counterfeit Electronic Components

Recommendations on Policies and Implementation Strategy

Henry Livingston, BAE Systems Electronic Solutions

INTRODUCTION

Counterfeit electronic components can jeopardize the performance, reliability, and safety of defense products. Over the past several years, increasing amounts of counterfeit electronic components have been introduced into the supply chain. Given the increased complexity of the supply chain, extra diligence is needed to ensure that the authenticity and performance of critical parts and materials is not compromised.

In a recent letter sent to the Department of Defense (DOD), Senator Tom Carper (D-Del.) and Senator Sherrod Brown (D-Ohio) urged the Administration to address the issue of counterfeit parts infiltrating the DOD supply chain[1]. This paper offers recommendations concerning policies and processes that the DOD and industry could employ to prevent the use of counterfeit electronic components and for detecting, reporting and tracking counterfeit electronic components.

THE BEST PROTECTION AGAINST COUNTERFEITS

From our own experience[2], undertaking the following steps may effectively combat counterfeit electronic components as they exist today.

Avoid risky sources of supply

The most effective approach to avoiding counterfeit electronic components is to purchase electronic components, where possible, directly from the original manufacturer, or from a distributor, reseller or aftermarket supplier that is franchised or authorized by the original manufacturer. The vast majority of counterfeit electronic components identified to date were procured at some point in the supply chain from independent distributors (i.e., those distributors who are neither authorized or franchised by the original component manufacturer for the parts they sell) and/or 'brokers'[i]. When purchases from sources of supply other than the original component manufacturer and its authorized distribution chain are necessary, due diligence must be performed to avoid counterfeits (product traceability, risk mitigation, verification / detection). When counterfeits are discovered, steps must be taken to avoid reintroducing counterfeits into the supply chain (containment, disposition).

Notify Government and Industry of suspect counterfeits encountered

When specific suspect counterfeits are encountered, these events should be promptly communicated both to Government and to industry. A recent Department of Commerce, Bureau of Industry and Security study[3] suggests that the incidence of counterfeit electronic components being found is under-reported by Government and industry. Sharing this information in a broadly accessible forum, such as the Government-Industry Data Exchange Program (GIDEP)[ii], enables other purchasers of the same or similar components to learn of this finding in near real time and be able to (a) examine their inventories and quarantine any questionable materiel they identify as well as (b) to check their open purchase orders to ascertain whether or not such components may be on order from the same or similar sources of supply.

Publicize the issue

Concerns surrounding the counterfeit electronic components issue and policy and processes applied to combat the problem should be publicized. We have found varying levels of awareness of the problem (and its impact) within the DOD and the contractor supply chain. Since a uniform and universal understanding of the issue is necessarily required to effectively combat this problem, DOD and industry concerns should use the many and effective avenues available to communicate these concerns.

POLICY AND IMPLEMENTATION STRATEGY CONSIDERATIONS

Defense products are prime targets for counterfeiters of electronic components. Defense systems are intended for use over extended time, leaving them vulnerable to obsolescence of parts, materials, subsystems, and technologies. As the length of time in use increases for a system, it is often challenging to obtain electronic components designed years

[i] Data sources include (1) "Defense Industrial Base Assessment: Counterfeit Electronics," U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, http://www.bis.doc.gov/, January 2010; and (2) The Government Industry Data Exchange Program (GIDEP).

[ii] The Government-Industry Data Exchange Program (GIDEP) is a cooperative activity between government and industry participants seeking to reduce or eliminate expenditures of resources by sharing technical information essential during research, design, development, production and operational phases of the life cycle of systems, facilities and equipment. (http://www.gidep.org/)

ago when replacements are needed to support fielded and new systems. The difficulty of avoiding counterfeit parts and materials occurs when defense contractors and the government are obliged to purchase parts from other than the original manufacturer (which may no longer manufacture them) or their authorized distributors.

Recent studies reveal that electronic components (such as microelectronics) currently present the greatest counterfeiting risk to DOD. A recent Department of Commerce, Bureau of Industry and Security study[4] includes information on the extent of the infiltration of such counterfeits. The data gathered for this study show that microelectronics comprised the majority of all reported counterfeit cases between 2005 and 2008[iii]. GIDEP data also show that the majority of counterfeit case reports concern microelectronics[iv]. Rather than establishing broad policies and practices that encompass all materiel commodities, we suggest that the near term policies and practices should: 1) focus on electronic components, 2) call for routine assessment of trends to determine the extent to which other materiel commodities emerge as a significant counterfeiting risk, 3) broaden the scope of policies and practices based on trend assessment results. This will enable existing resources to be directed to where significant risks presently lie and avoid diluting the execution of, and effectiveness of, the policies and practices by casting too wide a net.

When forming policies and practices, the following elements identified by Industry and US Government subject matter experts should be considered:

Procurement Practices and Supplier Selection

Policies and practices should emphasize the importance of procurement practices and product traceability over individual component verification and detection methods. Current industry and Government inspection and test methods are designed to verify the integrity and performance of authentic parts; not to detect counterfeits. While adjustments to and combinations of these methods can detect suspect counterfeits, they are not foolproof. Some counterfeit electronic components case reports reveal that documentation that accompanied the parts, such as Certifications of Conformance and test reports, were not authentic.

The most effective approach to avoid introducing counterfeit electronic components into systems and products is not to purchase them in the first instance. Since, as we indicate, the evidence suggests that such suspect materiel enters the supply chain via purchases made from independent distributors and brokers, electronic components should be purchased, where possible, directly from the original manufacturer, or from a distributor, reseller or aftermarket supplier that is franchised or authorized by the original manufacturer.

It has been represented to us that some U.S. Government and industry organizations are constrained in their ability to 1) apply a preference for procurement from Original Component Manufacturer or their authorized/franchised distributors and 2) apply counterfeiting countermeasures when procuring from Independent Distributors. We are also aware of conflicting interpretations on whether or not FAR Part 6 permits the Government to exclude bidders who are not the Original Component Manufacturer or its authorized or franchised distributors from offering components. If FAR Part 6 is interpreted such that procurement activities are constrained from excluding bidders who are not the Original Component Manufacturer or its authorized or franchised distributors from offering components, then these organizations will be encumbered in their ability to limit procurements to those component suppliers best prepared to combat the counterfeit electronic components issue.

Policy and practices should include the following:

- Specify a preference for procurement of electronic components from Original Component Manufacturer (OCMs), their authorized / franchised distributors, or through suppliers that furnish electronic components acquired from OCMs or their authorized distributors.
- Specify extra measures to be undertaken and/or employed when procuring from independent distributors and brokers.
- Provide universal definitions for “counterfeit” as respects electronic components as well as for “franchised or authorized distributor”, “independent distributor” and “broker”[v].
- Review FAR Part 6 to determine the extent, if any, to which procurement activities are constrained from excluding bidders that are not the Original Component Manufacturer (OCM) or its authorized or franchised distributors from offering components.
- Issue written guidance to clarify the FAR Part 6 exception by (1) defining OCMs or their authorized or franchised distributors as “responsible sources” and (2) requiring components be obtained from a limited number of responsible sources.

Counterfeit Component Case Reporting

The defense and aerospace industries and the Government lack consensus on whether or not to share information on component counterfeiting incidents discovered within their organizations. Some U.S. Government and industry

[iii] Data furnished by the Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation.

[iv] Data furnished by the Government-Industry Data Exchange Program (GIDEP)

[v] SAE standard AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition includes definitions of these terms. (http://standards.sae.org/as5553/)

organizations require direction and guidance concerning the methodology for reporting counterfeit component incidents. Some federal investigators have advised companies not to report in certain instances or to delay reporting through information sharing mechanisms such as GIDEP.

The Aerospace Industries Association (AIA) Counterfeit Parts IPT conducted a survey of U.S. Government and industry organizations to identify the primary benefits from sharing information on counterfeit components, and to identify obstacles and encumbrances to information sharing. Survey results show that defense and aerospace industries and the Government benefit from sharing information on counterfeit components. The predominant benefits are:

1. Avoiding and intercepting counterfeits discovered by others
2. Identifying suppliers associated with sales of counterfeit electronic components
3. Learning about ways those organizations reporting suspect counterfeit electronic components discovered the problem

The results of the AIA Counterfeit Parts IPT survey identify the following predominant obstacles and encumbrances to information sharing:

1. Perception of supposed legal or liability issues (e.g., exposure to third party law suits)
2. Lack of business process to support information sharing outside of the organization

Polices and practices should include the following:

- Establish GIDEP as the repository for receiving and disseminating counterfeit case reports.
- Provide qualified, limited immunity from third party suits to contractors, Original Component Manufacturer (OCMs), and component suppliers that report in good faith suspect counterfeit components via GIDEP, and cooperate with each other in assessing whether or not a given item is counterfeit.
- Establish contractual requirements and presumptions to increase sharing of counterfeit electronic component findings in order to alert other potential users in the defense & aerospace industries, Government agencies, and law enforcement[vi].

Counterfeit Component Disposition

Written guidance is needed from Federal Authorities concerning the disposition of counterfeit parts in the event and organization should purchase products they suspect to be counterfeit. Defense companies are generally aware of laws prohibiting the knowing sale/distribution of counterfeit products. Defense companies, however, are uncertain as to which agencies to report the counterfeit parts, whether to alert Government and industry via GIDEP and whether to (a) retain such counterfeit parts for later review and investigation by the Government investigative agencies, (b) destroy them (which may preclude the Government or contractor, as the case may be, from obtaining a refund from the source which sold them), or (c) notify the source that they are counterfeit and returning them to that source for a full refund.

Policy and practices should include written guidance on what a U.S. Government or industry organizations' obligations are if they should purchase products they suspect to be counterfeit. This guidance should include the following:

- The appropriate Government agency to contact in each and every case.
- Guidance on communicating concerns and findings about suspect counterfeit products to the supplier of those items.
- Guidance on alerting U.S. Government and industry as to their findings through GIDEP, as well as guidance on participation in GIDEP as the vehicle by which Industry and Government organizations alert each other of counterfeiting cases.
- Guidance on whether to retain suspect items (and for how long), destroy them, or return them to their supplier.[vii]
- Guidance in the event the Government is conducting an investigation including (a) what the Government expectations are with respect to the care and handling of the suspect parts that the Defense Contractors or Defense Agency procurement organizations have retained and (b) specific instructions required for Defense Contractors or Defense Agency procurement organizations would be on

[vi] Examples of contractual requirements and presumptions to increase sharing of counterfeit electronic component findings would include:
One Notification to US Government. Notification to GIDEP discharges and relieves the notifier from all other notifications to the US Government except (i) for notice specifically required to DCMA in certain enumerated circumstances such as a formal contract requirement to provide such notification; and
(ii) for notice to the specific Government customer if the material has been purchased and either (x) already delivered and/or (y) charged off under a specific US Government contract.
Not Evidence of Admission of Breach/Default. The notification to GIDEP, and the GIDEP report, cannot be used as an admission of breach in any contract with the US Government or its prime contractors where the basis for the alleged breach is the purchase and/or delivery of the very non-compliant material which is the subject of the GIDEP report. Conversely, the absence of the filing of a GIDEP report within XX days of detecting a counterfeit under a given contract shall be presumed to be a breach of a Government contract (and/or any prime contract issued there under) if the contract in question clearly and affirmatively requires GIDEP reporting of such findings as a condition of contract compliance

[vii] Some organizations do not return the suspect products: (a) because they may be required for evidence if the Government later expresses an investigatory interest and (b) for fear that one of the upstream suppliers in the chain may subsequently attempt to sell them again. Others, however, consider suspect counterfeit parts to be "non-conforming" material and return them as such for a refund or credit.

how to secure and store the items and how long should they be retained.

Component Obsolescence

Defense and aerospace products are particularly vulnerable to counterfeit components due to component obsolescence. Microelectronics products, in particular, have life cycles far shorter than the defense / aerospace products that use them. When obsolete parts are not eliminated from product designs, independent distributors are often used to obtain components that are no longer in production. Industry reports show that the vast majority of counterfeit components have been acquired from independent distributors.

According to study conducted by the Semiconductor Industry Association (SIA)[5], most counterfeit parts are those that are 'hard to get' because the parts were out of production, or current production capacity could not keep up with demand. While changes to procurement practices will reduce the number of purchases from higher risk suppliers, the prominence of through-life support contracts will make component obsolescence a larger challenge and counterfeits a possibly bigger problem for DOD and defense companies in the future.

In order to reduce the likelihood of having to purchase parts through higher risk suppliers, defense electronics producers and their customers recognize the need to proactively manage the life cycle of electronic products versus the life cycles of the parts used within them. Customers, however, are constrained regarding their ability to support and fund approaches to eliminate the use of obsolete components.

Policies and practices should include the following:

- Support and fund approaches to eliminate or mitigate the use of obsolete components.
- Require proposals for production and support contracts to identify obsolete components and to establish a plan to assure trusted sources of supply, re-manufacturing, replacement, and/or redesign.
- Establish a program to escrow intellectual property (e.g., product design, fabrication and testing information) for discontinued products with a 3rd party US escrow agent and permit US manufacturers ("trusted sources") to access them in order to support continuing government requirements.
- Establish a program to consign or sell surplus material with original component manufacturer or franchised distribution traceability to a "trusted source" entity for downstream support of government contracts/delivered equipment.

Duties of Importers

New industry standards have been created to provide uniform requirements, best practices and methods to mitigate the risks of receiving and installing counterfeit electronic components. Use of industry standards, however, will not reduce the significant and increasing volume of counterfeit electronic components entering the DOD supply chain. Subject matter experts agree that the Intellectual Property (IP) rights holder is best qualified to determine if a product is authentic or not. U.S. Customs and Border Protection (CBP) must have the authority to consult IP and trademark rights holders (e.g., Original Component Manufacturers) for assistance in determining whether or not imported goods are authentic. The importers of electronic components must take steps to ensure authenticity of imported items to prevent counterfeits from continuing within the supply chain.

Policies and practices should support other US Government agencies to:

- Establish policies that would allow CBP the statutory authority to consult IP and trademark rights holders (e.g., Original Component Manufacturers) for assistance in determining whether or not imported goods are authentic. This would include allowing CBP to provide photographs of the complete components markings and other shipping artifacts to the Original Component Manufacturer who, in turn, would notify CBP of their assessment concerning the authenticity of the product.
- Assess the adequacy of laws governing duties of importers to accurately report the authenticity of their imported goods and require importers to certify to the US Government, as a condition of import, 1) the source of off shore supply/manufacture, and 2) the authenticity of imported items.

Disposal of Electronic Waste

Industry studies reveal that many counterfeit electronic components originate overseas as parts salvaged from electronic waste. The export of electronic waste and scrap to developing nations is "feedstock" for counterfeiters of electronic components. The U.S. and other countries that use electronic products must eliminate the ready supply of circuit boards into the counterfeiters' supply chain.

Policies and practices should support other US Government agencies to restrict the export of electronic waste to developing countries, but allow the export of non-working and used electronic equipment for repair provided that means are established that prevent such equipment and constituent material from falling into the hands of salvaging operations which, in turn, supply counterfeiters.

DOD AND INDUSTRY COLLABORATION

The Government Accountability Office (GAO) examined 1) DOD's knowledge of counterfeit parts in its supply chain, 2) DOD processes to detect and prevent counterfeit parts, and 3) commercial initiatives to mitigate the risk of counterfeit parts. In its recent report[6], GAO recommended that DOD leverage existing initiatives to establish anti-counterfeiting guidance and disseminate this guidance to all DOD components and defense contractors. The industry initiatives described in the GAO report touch several industry organizations and consortia[viii]. DOD and Industry collaboration discussions should include these organizations and industry stake holder representatives. In the case of counterfeit electronic components, Government and Industry studies reveal that distribution channels (e.g., independent distributors and 'brokers') tend to be where counterfeits first appear within the supply chain. In addition to the industry organizations identified in the GAO report, representatives from the component distribution industry ("franchised / authorized" and "independent") should also be included in these discussions.

An excellent example of DOD and Industry collaboration is the SAE International G-19 Counterfeit Electronic Parts Committee. The SAE G-19 committee developed Aerospace Standard AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition[7]. SAE-AS5553 was adopted on 31 August 2009 for use by DOD (adopting activity: Navy – AS). The committee included representatives from DOD, NASA, the US Department of Homeland Security, prime contractors, component manufacturers, contract assembly manufacturers, franchised distributors, independent distributors, and industry association representatives. The SAE G-19 committee has since expanded its collaboration efforts to pursue further standards activity to address the counterfeit electronic components issue, and to include international representatives.

A CASE STUDY

On 14 September 2010, Federal prosecutors in Washington DC unsealed an indictment charging a Florida pair with conspiracy, trafficking in counterfeit goods, and mail fraud[8]. The indictment alleges these individuals and others imported counterfeit integrated circuits from China and Hong Kong and sold them to the U.S. Navy, defense contractors and others, marketing some of these products as "military-grade." In its press release the United States Attorney's Office describes how "This case shows our determination to work in coordination with our law enforcement partners and the private sector to aggressively prosecute those who traffic in counterfeit parts." There were numerous customer complaints regarding the counterfeit integrated circuits sold by the defendants and others, including the following event described in the indictment:

> *"An August 2007 sale of 75 counterfeit National Semiconductor Corporation ICs to a company in California that was fulfilling a joint contract with BAE Systems Technology Solutions & Services and the Naval Air Warfare Center Aircraft Division ("NAWCAD"), Detection and Surveillance Branch, Integrated Logistics Engineering. The ICs were intended to be used for production of ship-based antenna equipment, the Identification Friend Foe ("IFF") system, which is used to determine an airplane's identification and intentions while in flight."*

This event associated with BAE Systems and NAWCAD is an example of how collaboration between DOD and industry can effectively combat counterfeit electronic components as they exist today:

(1) When purchases from sources of supply other than the original component manufacturer and its authorized distribution chain are necessary, due diligence must be performed to avoid counterfeits.

(2) When counterfeits are discovered, steps must be taken to avoid reintroducing counterfeits into the supply chain.

(3) US Government agencies, contractors, and lower tier suppliers should promptly communicate their findings of counterfeits they encounter.

The specific parts associated with this event were integrated circuits. The original component manufacturer of these parts discontinued production of this product in 1993. The only suppliers offering these parts were independent distributors and brokers. Schedule and funding constraints did not allow for design changes necessary to eliminate the obsolete part.

Before considering the use of parts acquired from an independent distributor or broker, BAE Systems recommended to NAWCAD that it apply counterfeit avoidance practices developed by BAE Systems. These counterfeit avoidance practices are included in SAE Aerospace Standard AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition. The counterfeit detection procedure included within these practices revealed that the parts were suspect counterfeit. BAE Systems discussions with the original component manufacturer confirmed that the parts were counterfeit. The counterfeit parts were immediately segregated and quarantined, and did not re-enter the DOD supply chain.

BAE Systems initiated a GIDEP Alert[9] to notify government and industry of this finding. NAWCAD notified

[viii] The following industry organizations are among those actively involved in various standards and awareness initiatives concerning counterfeit electronic components:
Aerospace Industries Association (AIA)
Independent Distributors of Electronics Association (IDEA)
SAE International
Semiconductor Equipment and Materials International (SEMI)
Semiconductor Industries Association (SIA)
TechAmerica

the Naval Criminal Investigative Service (NCIS) of this counterfeit part incident. The GIDEP Alert submitted by BAE Systems prompted NCIS to refer the case to the US Department of Justice for further investigation and prosecution.

CONCLUSION

Government and industry must be vigilant in order to avoid counterfeit electronic components. This vigilance requires a new partnership between DOD and industry and understanding of programmatic and technical risks throughout all levels of the DOD supply chain.

We believe, when developing policies and practices to address the counterfeiting threat, DOD and industry should consider the issues and recommendations described in this paper and drive changes necessary to (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.

Henry Livingston is an Engineering Fellow and Technical Director at BAE Systems Electronic Solutions. He leads and supports a number of BAE Systems activities associated with specifying components and evaluating their suitability for military and aerospace applications. 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 on burgeoning problem of counterfeit parts with the government and industry.

REFERENCES

[1] "Senators Carper, Brown (Ohio) Urge Administration to Address Counterfeit Parts Infiltrating Department of Defense Supply Chains", http://carper.senate.gov/, 6 August 2010.

[2] "Avoiding Counterfeit Electronic Components", IEEE Transactions on Components and Packaging Technologies, Vol.30, Iss.1, pp.187-189, March 2007.
"Avoiding Counterfeit Electronic Components – Part 2 Observations from Recent Counterfeit Detection Experiences", BAE Systems Information and Electronic Systems Integration Inc., May 2007.

[3] "Defense Industrial Base Assessment: Counterfeit Electronics," U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, http://www.bis.doc.gov/, January 2010.

[4] "Defense Industrial Base Assessment: Counterfeit Electronics," U.S. Department of Commerce, Bureau of Industry and Security, Office of Technology Evaluation, http://www.bis.doc.gov/, January 2010.

[5] "A Look at Counterfeit Integrated Circuits", Semiconductor Industry Association Anti-Counterfeiting Task Force, DMSMS Conference 2008. http://www.dmsms2010.com/2008/

[6] "Defense Supplier Base: DOD Should Leverage Ongoing Initiatives in Developing Its Program to Mitigate Risk of Counterfeit Parts", GAO-10-389, Government Accountability Office, http://www.gao.gov/products/GAO-10-389, March 2010.

[7] SAE standard AS5553 – Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition (http://standards.sae.org/as5553/).

[8] "Owner and Employee of Florida-based Company Indicted in Connection With Sales of Counterfeit High Tech Devices Destined to the U.S. Military and Other Industries – Counterfeit Integrated Circuits Sold to U.S. Navy and Defense Contractors", United States Attorney's Office, 14 September 2010

[9] GIDEP Alert ZS9-A-09-01