How to Become DFARS Compliant and Avoid Counterfeit Parts in the Defense and Aerospace Supply Chain

8 Supply Chain Factors Contractors Should Consider
Table of Contents

Introduction .................................................................................................................................1
Counterfeit Parts in the Defense and Aerospace Supply Chain ..............................................1
   Definition of a Counterfeit .......................................................................................................2
How Counterfeit Electronic Parts Enter the Supply Chain .....................................................3
   eWaste ..................................................................................................................................3
   Intellectual Property Theft ....................................................................................................3
   Suppliers May Unwittingly Stock Counterfeits ....................................................................3
DFAR Final Rule on Counterfeit Parts .......................................................................................4
8 Supply Chain Factors Contractors Should Consider ............................................................5
Contractor Strategies for Mitigating Counterfeit Electronics Risk ...........................................6
   Research new suppliers carefully, according to business risk .............................................6
   Toughen up terms and conditions for purchasing ...............................................................7
   Tighten quality control and testing procedures for incoming inventory ............................7
   Trust, but verify—audit your suppliers over time .................................................................7
   Report suspected counterfeit parts promptly ........................................................................8
Automated Data Collection Enhances Supply Chain Traceability ..........................................8
Lessons from the Food and Beverage Industry—Field-to-Fork Traceability ..............................9
The Benefits of Automating Traceability .................................................................................9
Conclusion ................................................................................................................................10
Introduction

A fighter jet suffers a critical system failure during flight...the guidance system in a defense battery fails to intercept incoming missiles...a naval ship at sea loses navigation abilities. These types of nightmarish possibilities worry both defense contractors and the Department of Defense (DOD). If counterfeit electronic parts make it through the supply chain and into a mission-critical military asset, the potential for a worst-case scenario increases.

In 2014, Massachusetts resident Pierre Picone pleaded guilty to selling counterfeit integrated circuits (IC) to the U.S. Navy over the course of five years. The stakes could not have been higher—Picone knowingly supplied counterfeit parts for use in nuclear submarines. According to the Department of Justice, he conspired with suppliers in China and Hong Kong to sell over 12,000 counterfeit ICs for millions of dollars. These counterfeits featured markings normally found on legitimate parts from “approximately 35 major electronics manufacturers, including Motorola, Xilinx and National Semiconductor.”

After several recent investigations revealed the extent of counterfeit infiltration in the defense supply chain, Congress took action, modifying the rules for contractors concerning detection and avoidance of counterfeit parts as part of the National Defense Authorization Act of 2012 (NDAA). Rules for contracting with the DOD are outlined in the Defense Federal Acquisition Regulation System (DFARS).

This paper will examine the scale of the counterfeit parts problem and what’s changed in acquisition regulations to try to address it. We’ll also provide questions and strategies to help contractors improve systems and processes for combatting counterfeit electronic parts in the supply chain.

Counterfeit Parts in the Defense and Aerospace Supply Chain

In May 2012, after a year-long investigation, the Senate Armed Services Committee (SASC) released a report about electronics counterfeits in the defense supply chain. The investigation unearthed 1,800 cases of “bogus parts” with a total number of suspect counterfeit parts exceeding 1 million. The SASC “discovered counterfeit electronic parts from China in the Air Force’s largest cargo plane, in assemblies intended for Special Operations helicopters, and in a Navy surveillance plane.”

---

Definition of a Counterfeit
According to DFARS 252.246-7007:

- **A counterfeit electronic part** is “an unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer, or a source with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, date code, or performance characteristics.”

- **A suspect counterfeit electronic part** is “an electronic part for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the electronic part is authentic.”

Based on its findings, the SASC formed eight conclusions, including:

- Most counterfeit electronic parts in the defense supply chain are sourced from China.
- Permitting contractors to recover costs as a result of their own failure to detect counterfeits was counterproductive to DODs goals.
- The defense industry routinely failed to report cases of suspect counterfeit parts.
- The defense industry’s “reliance on unvetted independent distributors” results in risks to national security and military personnel.  

Richard Meene, Director, PriceWaterhouseCoopers Advisory Forensic Services, Government Contracts Practice, sees the magnitude of the counterfeit electronic parts problem as “huge” for several reasons: “First, the amount of electronic counterfeit parts in the supply chain is estimated to be significant. Second, the economic effect of counterfeit parts proliferation artificially lowers prices and puts strain on businesses who supply electronic components to the government. Finally, the risk of loss due to the inclusion of a nonconforming part in critical defense infrastructure is major; just think of counterfeit components being included in the navigation system of a military fighter jet, or in the guidance and control system of a missile.”

---

4 Written correspondence from Richard Meene, Director, PricewaterhouseCoopers Advisory Forensic Services Government Contracts Practice, received via email, June 26, 2015.
How Counterfeit Electronic Parts Enter the Supply Chain

Counterfeit electronic parts can be outright non-functional fakes, mismarked new parts that are sold as more expensive or higher quality parts, or the result of design theft and unauthorized part manufacturing. The defense and aerospace industries use only a small fraction of the semiconductors produced globally, so most counterfeit electronic parts are intended for the consumer or business-to-business markets.

eWaste
It’s most common for counterfeiters to harvest the electronic circuit boards from a variety of electronic devices that have been thrown away. Counterfeiters then remove the tiny integrated circuits (ICs) or microchips off the circuit boards (often by banging them), sand or chemically strip off the manufacturer’s markings, clean the chips (often in a dirty river), then dry and apply fresh markings with new part numbers.5

With the correct part numbers and manufacturer’s markings, these counterfeits can be surprisingly difficult to identify and catch. Sometimes the price may seem too good to be true. But usually, only testing will reveal counterfeits. And unfortunately, counterfeits sometimes pass the initial tests.

Intellectual Property Theft
Another way counterfeit electronic parts can enter the supply chain is through the theft and subsequent modification of the original manufacturer’s intellectual property. The design or manufacturing process may be modified to produce the parts more cheaply, and increase profit for a sophisticated counterfeiter who is fabricating ICs.

These parts would function, but wouldn’t be built to specifications and could be more prone to fail under real-world conditions. The only way to know with absolute certainty what is inside a chip is to break it open and have a computer optically compare its contents with the original design using high-power microscopes. The cost of this testing may approach the cost of the original R&D to design the chip and would rarely be pursued outside of high-stakes legal cases concerning intellectual property.6

Suppliers May Unwittingly Stock Counterfeits
Debbie White is a senior director of product management for Deltek, an ERP software vendor designed for project-based businesses including government contractors. “You really have to validate your supply chain upfront,” she cautioned contractors. “You need to know your suppliers, and your suppliers have to know their suppliers. A lot of these counterfeit

6 Interview with Dr. William Osborne, electrical engineer, July 24, 2015
electronics have leaked into the supply chain and people didn’t know about it. The problem is even your suppliers and distributors could be carrying counterfeit parts.”

A 2010 report by the Bureau of Industry and Security (BIS) reinforced this supply chain weakness. The report noted that the industry has generally regarded authorized distributors as safe and unauthorized distributors as risky, however “OTE survey data shows that these preconceptions confuse the true nature of the counterfeiting problem. Many authorized distributors assume the parts they acquire directly from OCMs are legitimate and do not require testing. However, survey data shows that some authorized distributors also assume parts purchased outside of their OCM agreements are legitimate and do not require careful screening. This practice, combined with buying back excess inventory from customers, has introduced counterfeits into the inventories of authorized distributors.”

DFAR Final Rule on Counterfeit Parts

Congress responded to the counterfeit parts problem through a new rule in Section 818 of the NDAA. After public review and discussion, the final rule was published in May 2014 and can be found at DFARS 252.246-7007.

Compliance with this regulation requires all prime contractors (those subject to Cost Accounting Standards (CAS)) to establish an “acceptable counterfeit electronic part detection and avoidance system.” This requirement also flows down to subcontractors supplying electronic parts to prime contractors, including commercial off the shelf (COTS) parts, as well as any other components, parts or assemblies.

The full requirements of such a system can be found in DFARS 252.246-7007. Among other things, each system must have processes in place to:

- Train personnel
- Inspect and test electronic parts
- Trace parts through the supply chain and use unique identifiers
- Quarantine counterfeit and suspect parts
- Report counterfeit or suspect electronic parts appropriately
- Use the best choices for suppliers
- Stay informed of industry reports and current counterfeiting trends

Another big change for contractors focuses on the issue of financial liability if a counterfeit electronic part causes a failure of a delivered product. In the past, the cost of fixing a problem due to a counterfeit part could usually be passed to the government. Now, if the government finds that the contractor

---

7 Telephone interview with Debbie White, Senior Director of Product Management for Project Manufacturing, Deltek, conducted June 1, 2015.
failed to establish an adequate detection and avoidance system, the contractor may be liable for these costs. While replacing a microchip would not cost much, if it caused the failure of a large military asset, the associated costs could be staggering.

8 Supply Chain Factors Contractors Should Consider

Defense and Aerospace contractors have a particularly difficult situation with counterfeit electronic parts, because it often takes a long time to source and receive the specialized parts for these types of projects. Contractors urgently need a good process in place for researching new suppliers and an airtight purchasing system.

“The market’s been flooded with these counterfeit parts and contractors haven’t really known what they’re getting until the counterfeits get to a quality control level. At that point it’s too late,” White warned. “If I order a part that has six months lead-time and receive a counterfeit part, I’ve got a huge wait time before I can finish manufacturing my item.”

To help contractors strengthen systems and processes that prevent counterfeit electronic parts, White recommended considering the following questions:10

1. Does your supplier have proper procedures in place to prevent counterfeit parts from getting into its supply chain?
2. How confident are you that your distributors follow proper procedures in acquiring the parts they deliver to you?
3. Is your internal quality control team trained to spot counterfeit parts before they are received into your inventory?
4. Does your inventory system have the capability to “quarantine” or isolate suspected counterfeit parts?
5. Does your procurement system allow you to place vendors on hold while you investigate suspected counterfeit parts? Can it apply sanctions to vendors who have supplied counterfeits?
6. When you’re validating or approving a new vendor, what do you expect that vendor to produce for you (certifications, documentation) to ensure the vendor won’t supply you with counterfeit parts?
7. Do your inventory systems include the ability to perform full tracking and traceability back to the original purchase, supplier and manufacturer information?
8. If your processes do identify bad quality or counterfeit parts, what steps are taken to remove these parts out of your inventory immediately? In the longer term, how will you keep those parts out of your supply chain?

“...the contractor may be liable for these costs. While replacing a microchip would not cost much, if it caused the failure of a large military asset, the associated costs could be staggering.

8 Supply Chain Factors Contractors Should Consider

Defense and Aerospace contractors have a particularly difficult situation with counterfeit electronic parts, because it often takes a long time to source and receive the specialized parts for these types of projects. Contractors urgently need a good process in place for researching new suppliers and an airtight purchasing system.

“The market’s been flooded with these counterfeit parts and contractors haven’t really known what they’re getting until the counterfeits get to a quality control level. At that point it’s too late,” White warned. “If I order a part that has six months lead-time and receive a counterfeit part, I’ve got a huge wait time before I can finish manufacturing my item.”

To help contractors strengthen systems and processes that prevent counterfeit electronic parts, White recommended considering the following questions:10

1. Does your supplier have proper procedures in place to prevent counterfeit parts from getting into its supply chain?
2. How confident are you that your distributors follow proper procedures in acquiring the parts they deliver to you?
3. Is your internal quality control team trained to spot counterfeit parts before they are received into your inventory?
4. Does your inventory system have the capability to “quarantine” or isolate suspected counterfeit parts?
5. Does your procurement system allow you to place vendors on hold while you investigate suspected counterfeit parts? Can it apply sanctions to vendors who have supplied counterfeits?
6. When you’re validating or approving a new vendor, what do you expect that vendor to produce for you (certifications, documentation) to ensure the vendor won’t supply you with counterfeit parts?
7. Do your inventory systems include the ability to perform full tracking and traceability back to the original purchase, supplier and manufacturer information?
8. If your processes do identify bad quality or counterfeit parts, what steps are taken to remove these parts out of your inventory immediately? In the longer term, how will you keep those parts out of your supply chain?"
**Contractor Strategies for Mitigating Counterfeit Electronics Risk**

Defense and aerospace contractors need to implement process improvements to avoid, detect, and trace counterfeit parts in the supply chain. The following strategies tie into specific DFARS system requirements. In addition to reviewing processes, contractors may need to strengthen aspects of their purchasing, inventory control, and other IT systems in order to be confident of their compliance with DFARS.

**If possible, order from original manufacturers or authorized partners**

The DOD recommends purchasing electronic parts from original manufacturers or “sources with the express written authority of the original manufacturer or current design activity, including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources.” Although purchasing electronic parts from the original manufacturer is the safest way to avoid counterfeits, there are many instances when contractors cannot source parts in this manner.

Most military aircraft have a service life of more than 40 years. During that time, the computers used to support the aircraft will change nine or more times, and its software will change at least three times. Most military aircraft have a service life of more than 40 years. During that time, the computers used to support the aircraft will change nine or more times, and its software will change at least three times.11 The aerospace industry association therefore concludes that, “supporting aerospace and defense products throughout their lifecycle sometimes requires the use of parts that may no longer be available from the Original Component Manufacturer (OCM), original equipment manufacturer (OEM), authorized aftermarket manufacturer or through franchised or authorized distributors or resellers.”

Meene pointed out that although the government wants to reduce costs, parts sourced through OEMs usually come with a premium price tag. And as platforms mature, OEMs often stop producing parts. Contractors must then rely on after-market parts manufactured by another company or surplus original parts; both types are sold primarily on the riskier gray market. “This will result in companies changing the manner in which they make final buys as procuring from a trusted source. Keeping a sufficient supply of clean inventory will be important,” he said.12

**Research new suppliers carefully, according to business risk**

Meene advises contractors to determine the depth and breadth of their new vendor research based on the amount of business risk that may be incurred. For example, in the purchase of a small quantity of parts for non-critical systems from a new supplier, simple open source research to determine the supplier is a legitimate company with proper licensing and a physical location maybe sufficient.

---

12 Written correspondence from Richard Meene, Director, PricewaterhouseCoopers Advisory Forensic Services Government Contracts Practice, received via email, June 26, 2015.
When the stakes are higher, due diligence should align with perceived business risk. For highly sensitive projects, research might include a site visit to look for signs of counterfeiting operations, reviews of the supplier’s purchasing and counterfeit detection systems, and deeper background on the officers and owners.13

**Toughen up terms and conditions for purchasing**
Contractors require a solid purchasing system, and DCMA routinely conducts Contract Purchasing System Review audits to ensure purchasing process integrity. With the new DFARS rule for counterfeit detection and avoidance, contractors need to employ tougher, more explicit terms and conditions in their purchase orders (PO) to suppliers. For example, contractors can specify they'll only accept certain brands of parts, obtained from original manufacturers.14 Terms and conditions should also require suppliers to maintain their own “acceptable counterfeit electronic part detection and avoidance systems” in compliance with the flow through application of the DFARS rule.

**Tighten quality control and testing procedures for incoming inventory**
An important part of the detection and avoidance system involves preventing counterfeits from making it into inventory by catching them at receiving. Contractors may need more robust quality control and testing procedures for electronic parts.

First, it may be necessary to have an inventory system with the ability to put parts “on hold” during receiving until the parts can pass quality checks. This way, untested parts can’t mistakenly get into production. It's also helpful to be able to isolate any suspected counterfeits in the inventory system while waiting for a supplier remedy.15

Parts should be visually inspected for obvious signs of counterfeiting, including sanding marks, polymer fillers, bent leads, and markings or artwork that don’t match the manufacturer’s product sheet.16

Meene suggests inventory testing plans, like new supplier research, should be based on the level of perceived business risk. When a contractor receives parts directly from an OEM, a limited testing protocol may be appropriate. For riskier supply situations, testing should be more extensive. It could include performance testing, and perhaps x-ray examination against specifications or even destructive testing that consumes a sample of the parts.17

---

13 Telephone interview with Richard Meene, Director, PricewaterhouseCoopers Advisory Forensic Services Government Contracts Practice, conducted July 1, 2015.
14 Telephone interview with Debbie White, Senior Director of Product Management for Project Manufacturing, Deltek, conducted June 1, 2015.
15 Telephone interview with Debbie White, Senior Director of Product Management for Project Manufacturing, Deltek, conducted June 1, 2015.
17 Written correspondence from Richard Meene, Director, PricewaterhouseCoopers Advisory Forensic Services Government Contracts Practice, received via email, June 26, 2015.
Trust, but verify—audit your suppliers over time
Sometimes a contractor has to use a supplier who is not an original manufacturer or an authorized sales partner. After doing research and establishing a business relationship, contractors should also have a system in place to monitor performance over time, making certain that the supplier does not switch to a less reliable part or a counterfeit part after making initial deliveries of legitimate parts.⁸

Report suspected counterfeit parts promptly
Contractors should ensure they have an internal process in place for reporting suspected counterfeits to the Contracting Officer and to the Government-Industry Data Exchange Program (GIDEP), as required by DFARS. Personnel should be trained on the proper way to report, and there should also be a process for getting the purchasing team involved in order to pursue remedies with the parts supplier.

Automated Data Collection Enhances Supply Chain Traceability
Supply chain process and technology improvements must address the core issue of traceability. Under the new DFARS rule, contractors must put in place “processes for maintaining electronic part traceability (e.g., item unique identification) that enable tracking of the supply chain back to the original manufacturer, whether the electronic parts are supplied as discrete electronic parts or are contained in assemblies."

“There’s just so much traceability that contractors have to do to be compliant on defense projects,” explained Debbie White. “They need to track through the product genealogy or as-built configuration, which goes down to the level of serial and lot information. Contractors really have three different bills of materials: as-engineered, as-manufactured, and as-built. It’s not cookie cutter stuff. You need to have traceability that goes along with it. If counterfeits do get into a finished product and it comes down to penalties, contractors risk losing their contract, if nothing else. That could put some contractors out of business.”

The DOD leaves contractors with the flexibility to decide what system to use for traceability. In analyzing the DFARS requirements, legal firm Crowell Morning noted “the contractor’s processes must, however, include certification and traceability documentation; clear identification of the name and location of supply chain intermediaries from the manufacturer to the direct source of the product for the seller; and, where available, the manufacturer’s batch identification for the electronic parts, such as date codes, lot codes or serial numbers.”¹⁹

“Contractors really have three different bills of materials: as-engineered, as-manufactured, and as-built. It’s not cookie cutter stuff. You need to have traceability that goes along with it.”

~ Debbie White
Senior Director of Product Management for Project Manufacturing
Deltek

---

Covington & Burling, LLP further cautioned “[a]lthough there is no mandated traceability technology, the preamble to the final rule notes that ‘[w]ith regard to mission-critical electronic parts that could impact human safety, DOD does have a zero-tolerance policy.’ The rule does not define what qualifies as an ‘impact [on] human safety’ or what consequences may be imposed for failure to meet that standard.”

Lessons from the Food and Beverage Industry—Field-to-Fork Traceability

As defense and aerospace contractors make decisions about the type of traceability system to put in place, they may want to examine the practices of another industry with a direct impact on human safety—the food and beverage industry. Just as a failed microchip could have harmful or even fatal consequences in a safety-critical defense system, food containing harmful ingredients or tainted by certain bacteria can cause illness or death for consumers.

High profile recalls of tainted food led to more stringent traceability requirements in federal regulations such as the 2001 Bioterrorism Act and the 2011 Food Safety Modernization Act. Feed, food and beverage manufacturers need to be able to trace each piece of produce or type of ingredient from “field to fork.”

Their traceability systems need to capture lot numbers, country of origin, and production information that can identify the grower/manufacturer, product, and even the location of the original field in the event of a recall. During food recalls, every hour is critical.

Consumers purchase and eat food quickly—especially fresh foods like produce and meat. Tracing individual lots using a manual paper trail would take too long. Automated data collection with mobile barcode scanners is being used in this industry to reduce the time to perform a recall from days to hours, potentially saving lives and controlling brand damage.

The Benefits of Automating Traceability

At many companies, traceability is a manual, paper-based process. If a counterfeit part is discovered coming into inventory, a contractor needs to respond quickly—isolating that part and any others like it. However, tracking counterfeit parts through a paper trail is usually a slow and tedious process.

An automated data collection solution reduces manual errors and speeds up traceability. Using barcoding or RFID and mobile handheld scanners, employees can track and trace inventory as it moves into and through the supply chain. With an integrated automated data collection solution, information in a contractor’s ERP system can be updated in real-time during receiving, testing, internal transfers, manufacturing, and order fulfillment.

For example, as a shipment of ICs is received from a supplier, employees use handheld barcode scanners to instantly capture date information and lot and serial numbers, before passing the parts on for identification, verification and testing. If an electronic part is suspected to be counterfeit, employees can quickly isolate that inventory with another scan to capture data. On the other hand, if an IC is accepted into inventory, traceability information will follow it through each stage of production, as it gets added to components and part assemblies and finally becomes part of a finished and delivered product.

Mobile data collection results in greater efficiency and visibility in the warehouse, store room, shop floor, plant, or even out in the field or shipyard. Automated data collection increases accuracy dramatically over a paper-based process. If a contractor needs to respond to an audit, automated data collection can trace items in minutes that might take hours or days to track down by paper invoices and purchase orders. To fully automate the traceability process, it’s important to select a mobile data collection solution with approved integration to existing ERP, inventory control, and/or purchasing systems.

**Conclusion**

When lives are at stake and national security may depend upon the quality of a work product, there’s no place for counterfeit, substandard parts. The final rule published at DFARS 252.246-7007 mandates that prime contractors and their subcontractors must establish a system for the detection and avoidance of counterfeit electronic parts. The DOD and contractors are working together to eradicate counterfeit electronic parts from the defense and aerospace supply chain.

This paper has outlined strategies suggested by the DOD and other supply chain experts for minimizing supply chain risks, including establishing an airtight system for tracing parts all the way back to the original manufacturer.
As with other highly regulated industries that impact human safety, defense contractors can benefit from a mobile data collection solution to enhance tracking and traceability of parts in the supply chain. A mobile data collection solution can provide the ability to automate traceability throughout the supply chain, rapidly identify and report suspected counterfeit parts, and comply quickly with traceability audits. As part of a larger system and process, it can be an important demonstration of DFARS compliance.

**RFgen Software—The Mobile Data Collection Experts**

RFgen Software helps organizations reduce supply chain implementation costs and increase accuracy and efficiency with the industry’s most reliable and flexible wireless and mobile automated data collection (ADC) software and open source supply chain solutions.

In business since 1983, RFgen is known in the manufacturing and distribution industry for its solid, high-quality products and high customer satisfaction ratings among its more than 2,800 customers. With a global reach and local touch, RFgen and its network of more than 140 certified solution partners can service and support your organization no matter where you’re operations are located around the world.

Using RFgen, businesses are able to quickly take their current manual processes and turn them into real-time mobile applications using barcoding, RFID, mobile and voice technologies. RFgen’s Mobile Foundation Suites accelerate the integration of mobile and barcoding technologies into your environment providing certified solutions that can simplify existing processes as well as combine multiple ERP operations into an optimized workflow.

Whether you are looking for solutions to automate your warehouse and better manage your inventory, comply with government regulations, ensure 24/7 warehouse operations, track and trace your products, voice-enable your warehouse, or manage your remote inventory, RFgen is the smart choice.

**To learn more, please call us at 888-426-2286, or visit our website at:**  