AEROSPACE REPORT NO.
TOR-2014-02200

Counterfeit Parts Prevention Strategies Guide

June 24, 2014

David C. Meshel
Joint Space Protection
GEOINT Futures Office

Prepared for:

National Reconnaissance Office
14675 Lee Road
Chantilly, VA 20151-1715

Contract No. FA8802-14-C-0001

Authorized by: National Systems Group

Developed in conjunction with Government and Industry contributions as part of the U.S. Space Program Mission Assurance Improvement Workshop.

Executive Summary

The proliferation of counterfeit electric, electronic, electro-mechanical, and electro-optical (EEEE) parts, hereafter referred to as "electronic parts," detected within the United States government supply chain has increased dramatically in the last five years. The volume and sophistication of counterfeit parts is steadily increasing and has been found in almost every sector of the aerospace and defense industry. Across the industry there has been a 250% increase in suspected counterfeit cases between 2005 – 2008[1] with another 4X increase between 2009 – 2012.[2] If counterfeit parts infiltrate the procurement system and are delivered in government products, they pose significant performance, reliability, and safety risks to the end user. In response to this mounting threat the President signed the 2012 National Defense Authorization Act (NDAA). Section 818 of the NDAA requires specific actions by contractors to eliminate the potential for procurement and utilization of counterfeit parts in any Department of Defense (DOD) system and places strict financial liability on the contractor for any impacts caused by counterfeit parts discovered in the product with only a limited safe harbor.[3]

The best defense against the proliferation of counterfeit parts is a proactive and strategic approach that mitigates the risk through:

1. Obsolescence management
2. Maximizing use of low-risk suppliers
3. Enhancing part availability throughout a product's life cycle through methods such as identifying acceptable product substitutions and system redesign
4. Implementing robust testing and inspection measures when procuring from higher-risk suppliers.

To effectively accomplish these defenses, emphasis should be placed on up-front preventive strategies. Taken together, an effective obsolescence control program and the selection of an electronic part supplier are the most crucial actions a contractor can make towards the elimination of the counterfeit part threat. A study of Government-Industry Data Exchange Program (GIDEP) documents over the past five years shows that over 99% of all suspected counterfeit cases resulted from the procurement of parts from a source <u>other</u> than an "authorized supplier" [Original Component Manufacturer (OCM), OCM franchised distributor, or aftermarket manufacturer].[4] This data shows that by merely procuring parts from an authorized supplier, the supply chain could eliminate a significant portion of the counterfeit threat, which would warrant less stringent systems and procedures to be implemented.

However, there may be occasions where it becomes necessary to procure from an "unauthorized supplier" (independent distributor or broker) and the use of these "reactive" processes becomes necessary. Obsolescence and the subsequent lack of part availability are among the primary reasons that a contractor may have to procure from these high risk suppliers. Regardless of the reason, the risk of introducing counterfeit parts increases dramatically when this decision is made. At this point, the only defense available is to mitigate the risk to the greatest extent possible. Due to the higher risk involved with procuring from unauthorized suppliers, any decisions to use an unauthorized supplier

[1]Senator Charles Schumer press release dated July 25, 2011
[2]IHS, Inc. Pressroom, Electronic Component Counterfeit Incidents Continue Record Pace as the US Department of Defense Set to Update Acquisition Rules, October 2, 2012
[3]See 2013 NDAA, §833
[4]A review of Government-Industry Data Exchange Program (GIDEP) documents yielded 487 documents issued in the 5-year period from 2009-2013 for counterfeit parts with two (2) of these being from OCM franchised distributors.

should be reviewed and approved by senior level management. In addition to the proactive measures, this document provides guidance on specific risk mitigation techniques to ensure the parts acquired are authentic.

The prime and principal subcontractors from the Space Quality Improvement Council (SQIC) and Space Suppliers Council (SSC) who represent the contractors for National Security Space (NSS) and Civil Space sector expressed concern that the requirements contained within Section 818 of NDAA 2012 and in the proposed Defense Federal Acquisition Regulation Supplement (DFARS) rule, 48 CFR 246.870 language[5], posed a schedule and financial risk to their company's operations. These contractors raised this issue to the Mission Assurance Improvement Workshop (MAIW) leadership. The MAIW commissioned a team to develop a document that the contractor community can use as a guide to assist them in implementing a Counterfeit Detection and Avoidance System that meets the intent/requirements of Section 818 of the NDAA and the DFARS rule.

This document provides guiding principles and practices that when implemented, could help ensure that the contractor's counterfeit electronic part avoidance and detection system aligns to, and is compliant with the 2012 NDAA law and DOD regulations regarding counterfeit protection. The framework of this guidebook follows the Counterfeit Electronic Part Avoidance and Detection System elements outlined in the DFARS rule, 48 CFR 252.246-7007(c). This document is further differentiated from other existing industry standards in the following ways:

- It addresses preventative techniques in design, program management, obsolescence management, and procurement management to raise the potential for part availability at the authorized supplier.
- It provides lessons learned, best practices, observations, driving philosophies and case studies from government agencies, contractors, and recognized industry subject matter experts (SMEs) who have been refining counterfeit prevention strategies for years.
- It outlines key topics for building an effective training program and contains links to fully developed programs that can be evaluated and tailored for incorporation into a supplier's training suite.
- It provides recommendations on information that should be captured and forwarded from a law enforcement perspective.
- Implementation of recommendations and guidance provided in this document can also assist the supply chain in obtaining certification of their procurement systems to the DFARS rules.

This document is intended to be a valuable guide for all contractors and suppliers, regardless of tier, to facilitate implementation of an effective counterfeit electronic parts avoidance and detection system, thereby reducing risk within government products. By increasing awareness and fostering collaboration throughout the supply chain, the risk of inadvertently procuring and using counterfeit parts at any level within the supply chain can be prevented.

[5] DFARS Rule, 48 CFR 246.870 was released on May 16, 2014, which added three system criteria to the nine originally proposed and added new section 252.246-7007.

Acknowledgments

This document was created by multiple authors throughout the government and the aerospace industry. For their content contributions, we thank the following contributing authors for making this collaborative effort possible:

Scot Lichty (Co-Lead), Lockheed Martin Corporation
Dave Meshel (Co-Lead), The Aerospace Corporation
Carlo Abesamis, NASA
Ken Baier, Lockheed Martin Corporation
Barry Birdsong, MDA
Greg Hafner, Orbital
Lilian Hanna, Boeing
Mike Kahler, Ball Aerospace & Technologies Corporation
Henry Livingston, BAE Systems
Bob Ricco, Northrop Grumman Electronic Systems
Fred Schipp, MDA/Navy
John Walker, SSL
Michael Woo, Raytheon
George Young, Raytheon
Jackie Wyrwitzke (Program Committee Focal Point), The Aerospace Corporation

A special thank you for co-leading this team and efforts to ensure completeness and quality of this document goes to Scot Lichty (Co-Lead), Lockheed Martin Corporation.

The Topic Team would like to acknowledge the contributions and feedback from the following organizations:

Aerojet Rocketdyne
The Aerospace Corporation
Area-51 ESG
Avnet
BAE Systems
Ball Aerospace & Technologies Corporation
The Boeing Company
Defense Contractor Management Agency (DCMA)
DoD Acquisition, Technology & Logistics (AT&L) / RESE GIDEP Program
Department of Justice (DOJ)/Computer Crimes & Proprietary Information Section (CCPIS)
Flextronics
Harris Corporation
Integra Technologies
Lockheed Martin Corporation
Micropac
Missile Defense Agency (MDA)
Moog Inc.
National Aeronautics and Space Administration (NASA)
Northrop Grumman Aerospace Systems
Orbital Sciences Corporation
Raytheon
SMT Corporation

Space and Missile Systems Center (SMC)
SSL
TTI, Inc.

The authors deeply appreciate the contributions of the subject matter experts who reviewed the document:

John Adams, The Aerospace Corporation
Gerald (Jerry) Aschoff, The Boeing Company
Sultan Ali Lilani, Integra Technologies LLC
Bob Bodemuller, Ball Aerospace & Technologies Corp.
Christopher Brust, DCMA
Shawn Cheadle, Lockheed Martin Corporation
Jim Creiman, Northrop Grumman
Dave Davis, SMC
David Ford, Flextronics
Dale Gordon, Aerojet Rocketdyne
Larry Harzstark, The Aerospace Corporation
Brian Hughitt, NASA
Yehwan Kim, Moog
Mark King, Micropac
James Koory, Aerojet Rocketdyne
C. J. Land, Harris Corporation
Jim Loman, SSL
Miroslav Maramica, Area-51 ESG
Terita Norton, The Aerospace Corporation
Ed Ortiz, The Aerospace Corporation
Michael Sampson, NASA
Don Sawyer, Avnet
Tom Sharpe, SMT Corp.
Kevin Sink, TTI, Inc.
Anduin Touw, The Boeing Company

Contents

Figures

Tables

1. Introduction

1.1 Purpose

The purpose of this document is to provide guiding principles and practices, that when implemented, will help ensure that the contractor's counterfeit electronic part avoidance and detection system effectively prevents and/or detects the purchase of counterfeit electric, electronic, electro-mechanical, and electro-optical (EEEE) parts, hereinafter referred to as "electronic parts," and is consistent with the Fiscal Year (FY) 2012 National Defense Authorization Act (NDAA), Section 818, the Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) rule, 48 CFR 252.246-7007.

1.2 Application

This guidance, when implemented, will help ensure that counterfeit electronic parts do not infiltrate the aerospace industry supply system and be installed in deliverable flight and ground space products. This guidance can also be used to establish and strengthen counterfeit prevention systems throughout the supply chain.

This document is intended for program management, procurement, legal, and technical disciplines to include engineering, production and quality organizations responsible for the creation and maintenance of counterfeit prevention systems. The guidance provided in this document incorporates key industry best practices and standards and applies them to the requirements of the DFARS. This document applies to the procurement of electronic piece parts and assemblies containing electronic piece parts intended for use in space applications, including spacecraft, launch vehicles, ground support equipment, and test and launch facilities. This document applies to new acquisitions, as well as repair, maintenance, and modernization services. This document applies to depots and arsenals, third party sources, and other value added services. While this document was written with space application in mind, portions of this document may be suitable for other users.

Appendix E portrays how this guide fits in with FY2012 NDAA, §818, DFARS rule, 48 CFR 252.246-7007, military specifications and industry standards.

1.3 Exclusions

This document does not address tampering and other malicious threats to hardware products containing electronic parts.

1.4 Terms and Definitions

The following are the key terms and definitions for readers of this document. This list is primarily based on terms and definitions found in DFARS rule, 48 CFR 252.246-7007(a) and SAE International AS5553, *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*. Customizations of definitions for use in this document are noted in the list. AS5553 should be referenced for an extensive list of terms and definitions.

Term	Definition
Counterfeit Electronic Part	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 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. (Source: DFARS rule, 48 CFR 252.246-7007(a))
Suspect Counterfeit Part	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. (Source: DFARS rule, 48 CFR 252.246-7007(a))
Electronic Part	An integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly. (Source: DFARS rule, 48 CFR 252.246-7007(a) with Team modification)
Electric, Electronic, Electro-mechanical, and Electro-optical (EEEE)	EEEE parts, hereinafter referred to as "electronic parts," are components designed and built to perform specific functions, and are not subject to disassembly without destruction or impairment of design use. Examples of electrical parts include resistors, capacitors, inductors, transformers, and connectors. Electronic parts include active devices, such as monolithic microcircuits, hybrid microcircuits, diodes, and transistors. Electro-mechanical parts are devices that have electrical inputs with mechanical outputs, or mechanical inputs with electrical outputs, or combinations of each. Examples of electro-mechanical parts are motors, synchros, servos, and some relays. Electro-optical parts include lasers, laser diodes and laser modules, light emitting diodes, light emitting modules, photo-detectors, photodiodes, photo-detector modules, optical transmitters and receivers and external modulators. (Source: AS5553 for EEE, Telcordia GR-468-CORE for electro-optical).
Authorized Supplier	Either the OCM or a distributor that has been reviewed and approved by the OCM and is under contract to distribute its parts or an aftermarket manufacturer possessing intellectual property rights received from the OCM for the part in question. An authorized supplier can be referred to as a Franchised Distributor. (Source: Team definition)
Original Component Manufacturer (OCM)	An organization that designs and/or engineers a part and is pursuing or has obtained the intellectual property rights to that part. (1) The part and/or its packaging are typically identified with the OCM's trademark. (2) OCMs may contract out manufacturing and/or distribution of their product. (3) Different OCMs may supply product for the same application or to a common specification. (Source: AS5553)
Original Equipment Manufacturer (OEM)	A company that manufactures products that it has designed from purchased components and sells those products under the company's brand name. (Source: AS5553)
Franchised Distributor	A distributor that performs authorized distribution, which is defined as transactions conducted by an OCM-Authorized Distributor distributing product within the terms of an OCM contractual agreement. Contractual Agreement terms include, but are not limited to, distribution region, distribution products or lines, and warranty flow down from the OCM. Under this distribution, the distributor would be known as an Authorized Distributor. For the purposes in this document, Franchised Distribution is considered synonymous with Authorized Distribution. (Source: AS5553 as modified by Team)

Term	Definition
Aftermarket Manufacturer	Products that are no longer available through the OCM or an OCM authorized distributor may be available through authorized aftermarket manufacturers. Aftermarket manufacturers generally fall within the following categories: authorized by the OCM or Intellectual Property (IP) holder to produce and sell parts, usually due to an OCM or IP holder's decision to discontinue production of a part, produces parts using semiconductor die or wafers, manufactured by and traceable to an OCM or IP holder, or produces parts through reverse-engineering that match the OCM or IP holder's specifications without violating the OCM or IP holder 's intellectual property rights and with the OCM or IP holder's authorization. While authorized aftermarket manufacturers play a vital role continuing supply once manufacturers discontinue products and authorized distributor inventory is depleted, use of aftermarket manufacturers is not a guarantee of support for all products needed, nor is it a guarantee of infinite supply for products they do support. (Source: AS5553 as modified by Team)
Approved Supplier	A supplier that has been subjected to and successfully passed a contractor's detailed evaluation requirements and has been deemed to have acceptable risk mitigation processes in place. (Source: Team)
Independent Distributor or Broker	A distributor that purchases parts with the intention to sell and redistribute them back into the market. Purchased parts may be obtained from OEMs or Contract Manufacturers (typically from excess inventories), or from other Distributors (Franchised, Authorized, or Independent). Resale of the purchased parts (redistribution) may be to OEMs, Contract Manufacturers, or other Distributors. Independent Distributors do not normally have contractual agreements or obligations with OCMs. See definition of Franchised Distributor. In the independent distribution market, Brokers are professionally referred to as Independent Distributors. (Source: AS5553)
Supply Chain Traceability	Documented evidence of a part's supply chain history. This refers to documentation of all supply chain intermediaries and significant handling transactions, such as from OCM to distributor, or from excess inventory to broker to distributor. (Source: AS5553)
Government-Industry Data Exchange Program(GIDEP)	GIDEP is a cooperative activity between government and industry seeking to reduce or eliminate duplicate expenditures of time and money by making maximum use of existing knowledge. The program provides a media to exchange technical information. (Source: GIDEP web page as modified by Team)
Contractor	For the purposes of this document "contractor" applies to government agencies and industry organizations. (Source: Team)

1.5 Overview

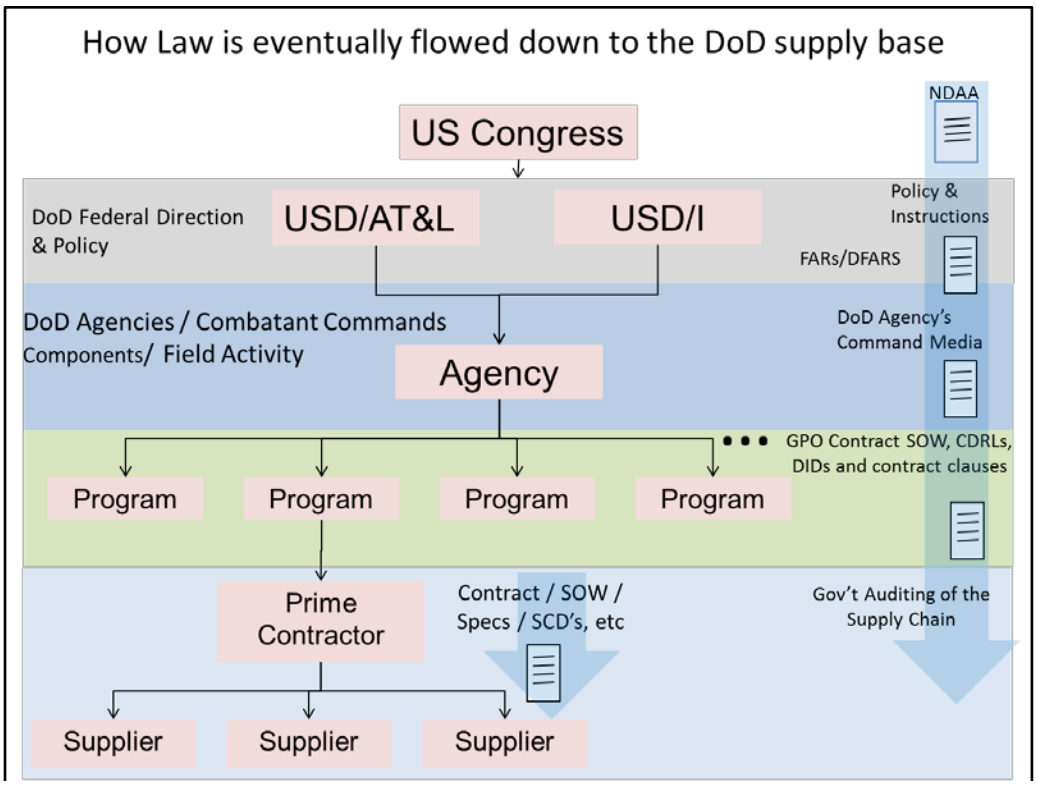
The proliferation of counterfeit parts within the United States government supply chain has increased dramatically in the last five years. Although this is an issue at all levels, the primary avenue for these parts to enter the supply chain is in the lower tiers, two or more levels separated from the prime contractor.[6] Reasons such as part obsolescence, cost constraints, and system sustainment may drive the supplier to purchase outside the authorized supply chain. Because prime contractors have limited visibility deep into the supply chain and limited resources to verify compliance at all levels, it is necessary to increase awareness and foster collaboration to reduce the risk of counterfeit electronic parts throughout the supply chain.

Due to this proliferation and threat to the Department of Defense (DOD) systems, Congress passed the FY2012 NDAA, §818.[7] The law includes an expectation for contractors to "establish policies and

[6] A review of Government-Industry Data Exchange Program (GIDEP) documents yielded 487 documents issued in the 5 year period from 2009-2013 for counterfeit parts with two (2) of these being from OCM franchised distributors.

[7] H.R.1540, National Defense Authorization Act For Fiscal Year 2012, Section 818(e), "Improvement of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts"

procedures to **eliminate counterfeit electronic parts from the defense supply chain**, which policies and procedures shall address … **processes to abolish counterfeit parts proliferation**" (emphasis added).[8] The DFARS rule, 48 CFR 252.246-7007, Contractor Counterfeit Electronic Part Detection and Avoidance System, establishes the system criteria for a counterfeit electronic part detection and avoidance system.[9] Figure 1-1 shows how a law is flowed down to the supply base.



- **NDAA** – National Defense Authorization Act. Law passed by Congress and signed by the President of the United States that defines what actions and policies the DOD is to enact starting that fiscal year of the NDAA.
- **USD/AT&L** – Under Secretary of Defense for Acquisition, Technology, and Logistics. This is the department within the DOD that has the overall responsibility for the procurement and fielding of DOD systems. They are responsible for the implementation of policies that are defined in the NDAA's and other government laws and regulations.
- **Agencies**. Agencies are those organizations that are responsible for the procurement of DOD systems of systems. USAF Space and Missiles Systems Center (SMC), National Reconnaissance Office (NRO), Missile Defense Agency (MDA), and Defense Logistics Agency (DLA) are examples of "Agencies" who procure systems of systems for the DOD.
- **Programs**. The actual government program office responsible for procuring a specific DOD system. For example within USAF/SMC, there are: Navigations System, MILSATCOM, Overhead Persistent InfraRed, and Weather and Space Situation/Protection Program offices that procure the actual satellite and ground equipment that comprise the system.
- **Prime Contractor**. The company responsible for the design, development, manufacture, assembly, test, qualification and deployment of the system being procured by the government program office.
- **Suppliers**. The term suppliers is used here in a broad sense meaning that any company that provides subsystems, units (black boxes), components (electronic parts), manufacturing or assembly/test services that are built into the system being delivered by the prime contractor are considered a supplier. Suppliers include subcontractors, sub-tier suppliers, and component providers and could be "authorized" or "unauthorized" suppliers.

Figure 1-1. How law is eventually flowed down to the DOD supply base.

The global nature of the supply chain presents significant barriers to eliminating counterfeit products from the supply chain altogether. While a contractor can implement policies and procedures to

[8] H.R.1540, National Defense Authorization Act For Fiscal Year 2012, Section 818(e), "Improvement of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts"
[9] DFARS rule, 48 CFR Part 252—Solicitation Provisions and Contract Clauses, subsection 252.246–7007, Contractor Counterfeit Electronic Part Avoidance and Detection System, (c).

prevent counterfeit parts it discovers from re-entering the supply chain, a contractor is not in an effective position to eliminate counterfeit parts proliferation throughout the supply chain. However, definitive countermeasures can be applied by contractors to manage this problem more effectively.

A contractor's Counterfeit Electronic Part Avoidance and Detection System should apply a strategy consistent with the DOD Counterfeit Prevention Policy.[10] This involves:

- Employing an end-user focused risk-based approach, such as described in AS5553 and NASA MSFC-STD-3619, to reduce the frequency and impact of counterfeit materiel within DOD acquisition systems and DOD life cycle sustainment processes
- Applying prevention and early detection procedures to minimize the presence of counterfeit materiel

Counterfeits tend to find their way into the supply chain through two primary paths:

- Procurement at any point in the supply chain from other than an authorized supplier
- Procurement from independent distributors without sufficient supplier selection and counterfeit avoidance/detection practices

A Counterfeit Electronic Part Detection and Avoidance System should incorporate the following central tenets recommended by industry and US government subject matter experts (SMEs):

- Apply supplier preferences for electronic components purchased from authorized suppliers
- Manage component obsolescence risks and engage customers to weigh assembly redesigns to eliminate obsolete parts versus counterfeit parts risk mitigation associated with acquiring parts from other than authorized suppliers
- Perform due diligence as outlined in this document to avoid counterfeits when purchases from sources of supply other than an authorized supplier are necessary
- When counterfeits are discovered, take steps to avoid reintroducing counterfeits into the supply chain
- Notify government and industry of suspect counterfeits when they are encountered
- Flow down and verification of the above tenets through all levels of the supply chain

Contractors and their sub-tier suppliers should incorporate and flow down key counterfeit avoidance and detection standards within compliance programs, including TOR-2006(8583)-5235, AS5553, AS6081, and AS6171 (draft).

The balance of this document offers guidance based on the twelve system criteria as described in the DFARS rule, 48 CFR 252.246-7007(c) for a contractor's Counterfeit Electronic Part Detection and Avoidance System. The twelve criteria are:

5. The training of personnel.
6. The inspection and testing of electronic parts, including criteria for acceptance and rejection.
7. Processes to abolish counterfeit parts proliferation.

[10]DODI 4140.67, DoD Counterfeit Prevention Policy (26 April 2013) at 3.b

8. Processes for maintaining electronic part traceability.
9. Use of suppliers that are the original manufacturer, 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.
10. The reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts.
11. Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit electronic part is, in fact, counterfeit.
12. Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts.
13. Flow down of counterfeit avoidance and detection requirements.
14. Process for keeping continually informed of current counterfeiting information and trends.
15. Process for screening the Government-Industry Data Exchange Program (GIDEP) reports and other credible sources of counterfeiting information.
16. Control of obsolete electronic parts.

1.6 National Security Space (NSS) Systems

Although there has been a proliferation of counterfeit parts in recent years this has not generally affected the space vehicles associated with NSS programs. This is partially due to the rigorous controls that are applied to the spacecraft procurements of parts, materials and processes (PM&P). The PM&P requirements are defined in TOR-2006(8583)-5235, which includes provisions for prevention and detection of counterfeit parts and materials. A portion of this document is based on lessons learned from PM&P Control Board (PMPCB) activities that have prevented counterfeit parts from penetrating the DOD space systems.

2. Design, Operation, and Maintenance of Systems to Detect and Avoid Counterfeit Electronic Parts

DFARS rule, 48 CFR 252.246-7007(c)(8) requires the "Design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts. The contractor may elect to use current government- or industry-recognized standards to meet this requirement."

The prime and sub-tier contractors should design, operate, and maintain a system to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts. Policies and procedures should be created for the purpose of identifying counterfeit and suspect counterfeit electronic components and preventing their inadvertent inclusion in delivered products. These policies and procedures should be incorporated as a system and implemented and adjusted over time to achieve their purpose.

Experience has shown reactive measures to be neither adequate nor cost effective. Proactive measures that prevent the procurement and use of counterfeit parts include: design, obsolescence management, source selection policies, program planning/schedule management, life cycle management, supply chain threat assessments[11], subcontractor/sub-tier supplier assessments, awareness and training and requirements flow down.

For most NSS programs parts, materials and processes procured or used are managed by the program's PMPCB as defined in TOR-2006(8583)-5235 (MIL-STD-1546). Specific to counterfeit mitigation the PMPCB approves all procurements from unauthorized suppliers (either approved or unapproved). In addition, the PMPCB is responsible for the reporting and investigation of any suspected or confirmed counterfeit parts detected within their program.

Past experience has also indicated that counterfeit electronic parts are as much the result of a lack of supply chain control as of the electronic system's design authority to actively monitor the obsolescence status of the bill of materials. The necessity to utilize unauthorized suppliers largely stems from insufficient pre-planning, resulting in either a long-lead-time hurdle for procurement, the realization that a part has gone out of production during a long break in procurement activity, or additional cost due to minimum buys and convenience. These issues may be avoided through the application of the following preventative measures:

- Active Management of Electronic Parts Obsolescence

  Proactive versus reactive electronic parts obsolescence management is the continuous monitoring of electronic part obsolescence as opposed to checking the availability of a part when stock is depleted. The assembly design authority accomplishes active obsolescence control by first identifying all electronic parts used and documenting these within a database. By applying electronic part obsolescence information to this database, it is then possible to identify the requirement for last-time-buys in order to ensure future availability of the parts before OCM production has ceased. This database can be either company internal or entrusted to a third party, but by actively monitoring the obsolescence status of electronic parts, it may be possible to completely avoid procurement from an unauthorized supplier.

  As a component of obsolescence management, the organization should be committed to preventive measures such as (1) procuring and maintaining a lifetime stock of critical electronic components, (2) conducting earlier design modifications and reviews, and (3)

[11] DoDI 5200.39, Critical Program Information (CPI) Protection within the Department of Defense

collaboration with critical discrete component [e.g., field effect transistors (FETs), diodes] manufacturers for sustained designs or earlier obsolescence notice, as required in order to ensure availability. Regular reviews of projected consumption should be maintained.

- Alternate Parts Review

  In the event of a shortage of parts, the organization should perform an alternate parts review prior to considering procurement from an unauthorized supplier. Alternative (drop-in) parts from authorized suppliers are preferred over procurement from an unauthorized supplier. Additionally, up-screening lower level parts from authorized suppliers is preferred over procurement from an unauthorized supplier. Ultimately, the organization should be willing to re-qualify designs as necessary to avoid the possibility of encountering a counterfeit part.

- Improved Production Planning

  Just-In-Time (JIT) inventory control is key to commercial profits, but in the aerospace industry, electronic part authenticity assurance is key to mission success and should take precedence. Improved production planning requires the foresight to allow for lead times for electronic part procurement through authorized suppliers.

- Realistic Delivery Schedules

  As with production planning, the aerospace industry needs to be aware of the pitfalls of placing pressure on delivery schedules that drive suppliers to look for out-of-the-box ways to meet schedules. By imposing unrealistic schedule requirements on suppliers, the likelihood of incurring an unexpected shortcut of brokered electronic part procurement is significantly increased. An attention to detail regarding procurement only from authorized suppliers should always take precedence over schedule.

An effective counterfeit parts mitigation system should be coordinated among all of the activities that are affected. Such a coordinated system can be designed based upon a standard such as AS5553 or AS6081, as applicable, and certified by a second or third party if appropriate.

The design of such a coordinated system is illustrated in Figure 2-1. Notice that the complete system covers all aspects of program management, design, and part procurement. It is important that a coordinated system addresses all of these areas in order to be effective.

When such a system has been implemented, it is critical that the utmost discipline be used in its operation. Lapses in vigilance and failure to follow the procedures are the most common causes of counterfeit part problems. The operation of the system should be constantly monitored and continuously improved as experience dictates.

The subsequent sections of this document will address the individual areas of the system as outlined below. The process outlined below should be engaged as early in the program planning, design, manufacture, operation, and maintenance of a system as possible.

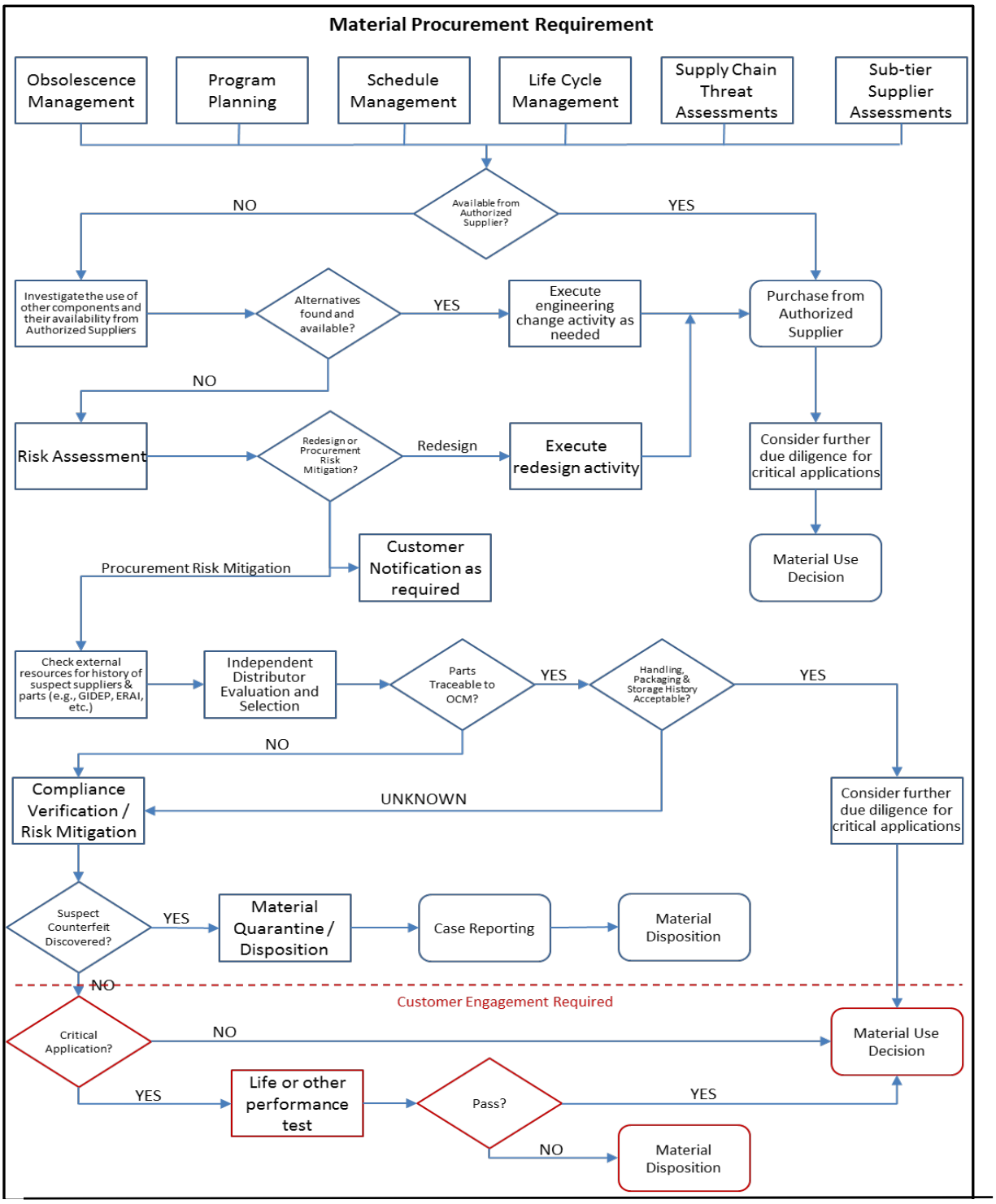


Figure 2-1. Coordinated counterfeit parts mitigation process.[12]

[12]This figure adapted from a similar figure in AS5553, *Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition*

2.1 Use and Approval of Suppliers

Section 3 discusses the use and approval of suppliers. The primary source of parts should be authorized suppliers. Unauthorized suppliers are considered to be at a higher risk for providing counterfeit product. If it becomes necessary for a contractor to choose an unauthorized supplier this section guides the supplier selection process. It is necessary to be knowledgeable about the suppliers chosen to evaluate the risk of using them and to take the necessary steps to assess and approve suppliers to mitigate any risk.

2.2 Mechanisms to Enable Traceability of Parts to Suppliers

Section 4 establishes an approach for requirements, polices, and activities for managing and implementing electronic part traceability.

2.3 Inspection and Testing of Electronic Parts, Including Criteria for Acceptance and Rejection

When procurement outside the authorized supply chain is necessary, the electronic parts should be inspected and tested to verify their authenticity. Section 5 discusses the steps recommended to provide the optimal counterfeit protection.

2.4 Reporting and Quarantining of Counterfeit Parts

Section 6 discusses the details of the quarantine and reporting of counterfeit parts. The FY2012 NDAA requires contractors that supply electronic parts or systems that contain electronic parts to establish policies and procedures to prevent counterfeit electronic parts from entering the defense supply chain. The fundamental objective of reporting is to minimize impact and maximize containment of the counterfeit item event and to notify stakeholders and interested parties of findings which may impact their operations or products.

2.5 Flow Down of Counterfeit Avoidance and Detection Requirements

Section 7 discusses the flow down of counterfeit avoidance and detection requirements as depicted in Figure 1-1. Requirements flowed down to suppliers should focus on the predominant means by which counterfeit electronic parts find their way into the supply chain and should embody the central tenets of counterfeit prevention.

2.6 Training of Personnel

Section 8 discusses the training of personnel. Counterfeit parts training serves a variety of purposes depending on the maturity and familiarity of the organization's counterfeit parts mitigation process. A solid training program will address general awareness and provide detailed expectations and requirements tailored to specific groups within the organization. Appendix A provides sample training resources for use and adoption throughout the supply chain.

2.7 Maintaining Currency on Counterfeiting Information and Trends

Section 9 discusses some methods and expectations for keeping continually informed on the evolving threat of counterfeit electronic parts.

3. Use and Approval of Suppliers

DFARS rule, 48 CFR 252.246-7007(c)(5) requires the "Use of suppliers that are the original manufacturer, 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. When parts are not available from any of these sources, use of suppliers that meet applicable counterfeit detection and avoidance system criteria."

Obsolescence control decisions and the selection of an electronic part supplier are the most crucial decisions a company will make towards the elimination of the counterfeit parts threat. Counterfeit parts tend to find their way into the supply chain through unauthorized suppliers.[13] Accordingly, the single most important practice downstream of obsolescence control is to procure electronic parts from authorized suppliers. If this practice is strictly followed, the counterfeit part risk may be restricted to obsolete parts and the rest of this document and many industry standards that describe reactive processes such as inspection, test, quarantine, and reporting may be unnecessary.

However, there may be occasions when the purchasing organization may need to procure from an unauthorized supplier. Obsolescence and the subsequent lack of part availability are among the primary reasons for procuring from these high risk suppliers. Regardless of the reason, the risk of introducing counterfeit parts increases dramatically when this decision is made. At this point, the only defense available is to mitigate the risk to the greatest extent possible. The remainder of this section provides guidance on how to select a supplier that maximizes the potential of acquiring authentic parts. Using any supplier other than an authorized supplier should be a measure of last resort, used only when all other avenues have been exhausted, and should be reported to the customer [e.g., as stated in TOR-2006(8583)-5235]. In fact, if an electronic part is proven to be unavailable from authorized suppliers and there is significant demand for future parts, the contractor should consider system redesign, qualification of replacement parts, or approach the OCM and ask if they would be willing to re-manufacture or re-constitute that product line in order to alleviate the issue. Another avenue is to contact Defense Microelectronics Agency (DMEA) to determine if they can manufacture an equivalent part using reverse engineering techniques.

There are multiple terms in the community that describe a supplier's pedigree and appropriateness for selection to supply electronic parts. Terms including "authorized," "qualified," "approved," "preferred," and "trusted" all exist and have subtle differences. Confusion exists as sometimes these terms are used interchangeably or inconsistently throughout the community depending on the contractor or customer. These terms are not created equally, and the fact that they sound similar (and positive) sometimes leads to a false sense of security for a purchasing organization. Since this is a guidance document (and not a standard), an attempt has been made to take a complex situation and make it simple, at the risk of leaving several of these terms and subtleties out of the discussion. In an effort to provide a basic framework example and to break it down into its simplest terms, only three terms will be used to describe suppliers: authorized, unauthorized, and approved.

An authorized supplier is the OCM, an OCM franchised distributor, or an aftermarket manufacturer. Authorized and franchised distributor information can be obtained from the OCM website, although the data may not always be current. The OCM should be contacted to obtain the most current list of franchised distributors for their product.

[13] A review of Government-Industry Data Exchange Program (GIDEP) documents yielded 487 documents issued in the 5 year period from 2009-2013 for counterfeit parts with two (2) of these being from OCM franchised distributors.

Note: The Semiconductor Industry Association promotes "The Authorized Directory"[14] as a resource for identifying authorized OCM distributors. The Electronic Component Industry Association (ECIA) maintains data for users to identify authorized sources (ECIAauthorized.com).[15] These sources may have limitations and further research may be needed to verify accuracy.

When parts are not available from an authorized supplier, another acceptable source of supply are those suppliers that meet applicable counterfeit detection and avoidance system criteria and only procure directly from authorized suppliers.

An unauthorized supplier is everyone else – all companies that are not contractually authorized by the OCM to sell their product. This includes all independent distributors and brokers that may carry the desired part. It is important to note that this simplification can still be complicated by the fact that a supplier may be authorized to sell one product from an OCM, but unauthorized to sell other products from the same OCM.

As stated earlier, if the purchasing organization needs to use an unauthorized supplier, a rigorous evaluation and assessment process can be conducted to increase the confidence in the unauthorized supplier, resulting in subsequent "approval" of that supplier for ongoing procurements by the purchasing organization, or to mitigate risk for a single procurement. Suppliers approved for ongoing procurements are those suppliers that have been assessed or audited by the appropriate contractor's organization, and have been determined to have continuously controlled processes to provide consistent delivery of authentic, reliable, and quality parts that conform to the contract or purchase order specification requirements.

An approved supplier can be an OCM, an authorized/franchised distributor, independent distributor or broker that has passed a number of assessments and evaluations designed to maximize the contractor's confidence that the supplier will deliver authentic, reliable product. An approved supplier should not be mistaken for an authorized supplier. Unauthorized suppliers that have been approved by the contractor for procurement may be considered a lower risk, but they are still unauthorized suppliers, and carry a higher risk for the introduction of counterfeit parts than an authorized supplier. Figure 3-1 depicts the authorized, unauthorized, approved supplier relationship. A subtle, but important difference is that the contractor approves an independent distributor through risk mitigation techniques, but only the OCM can authorize or franchise a distributor or aftermarket manufacturer. There is no mitigation technique that can be employed that lowers the risk of a contractor approved "unauthorized" supplier to that consistent with the OCM authorized supplier. This is why a contractor approved "unauthorized" supplier should only be used as a last resort and only if all means are exhausted to use an OCM authorized supplier.

The remainder of this section predominantly describes risk mitigation techniques, assessments, evaluations, and other strategies to approve and select an unauthorized supplier for procurement when authorized suppliers are not available. This section leverages value-added requirements and guidance from the DLA's Qualified Suppliers Listing of Distributors (QSLD) and Qualified Testing Suppliers Listing (QTSL) documents, as well as best practices identified by subject matter experts within the MDA, Navy, National Aeronautics and Space Administration (NASA), NRO, Army, Air Force, DLA, and Defense Contract Management Agency (DCMA).

[14] http://www.authorizeddirectory.com
[15] http://www.eciaauthorized.com/

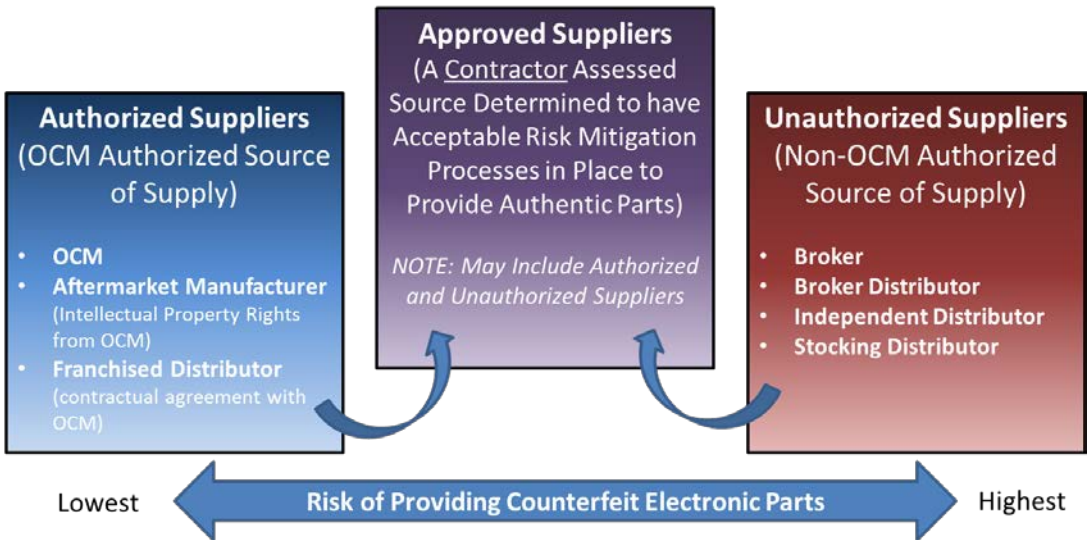


Figure 3-1. Suppliers – Authorized vs Unauthorized vs Approved.

3.1 Supplier Selection

When a contractor assesses or audits an unauthorized supplier with the intention of giving the company 'approved supplier' status, the supplier's own supplier selection, approval, avoidance, and reporting processes should be thoroughly checked for compliance with industry best practices or the contractor's own requirements. The remainder of this section addresses the review of an approved supplier's processes. These observations should form a part of the contractor's supplier assessment process. Appendix G provides a counterfeit parts process audit checklist example that may be used as a starting point in conducting a supplier assessment.

3.1.1 Authorized Suppliers

3.1.1.1 The contractor purchasing organization should have documented procedures to identify and differentiate between authorized and unauthorized suppliers. The determination if a supplier is authorized should be applied individually for each OCM and product line (i.e., a supplier should not be assumed authorized for all OCMs and product lines). OCM websites or OCM contact personnel should be used to determine the extent of the supplier's authority to sell parts. For example, an OCM that produces electronic parts for multiple product lines (e.g., diodes, transistors, different types of integrated circuits) might not have the same authorized suppliers for each product line.

3.1.1.2 The contractor purchasing organization should have documented procedures to ensure that all electronic parts are obtained directly from an authorized supplier, unless the parts are no longer in production by the OCM or aftermarket manufacturer, and residual stock is no longer available from franchised distributors. In cases where the organization can obtain parts directly from an authorized supplier, the authorized supplier should provide traceability documentation (Note: the buyer is encouraged to periodically confirm the documentation's authenticity). The buying organization should have processes in place that require senior level management approval (program, procurement, and quality managers at a minimum) before the buyer can purchase electronic parts from an unauthorized supplier.

3.1.1.3 If an authorized supplier cannot provide parts obtained directly from the OCM, the contractor should be informed, along with the name and address of the source of the parts to the authorized supplier. This notification and information should be provided at the time of quoting. Authorized

suppliers should not stock or sell parts received from unauthorized sources. This includes parts returned from a customer that are not in original factory-sealed packaging, as other parts may have been substituted.

3.1.1.4 If electronic parts are purchased from an approved authorized supplier who purchased those parts directly from the OCM, the parts can be assumed to be authentic without requiring any of the special actions described in the rest of Section 3.1. For even greater confidence, the contractor may require the authorized supplier to provide only OCM-direct, never-returned product and a Certificate of Conformance (CoC) signed by the OCM, or have the product shipped directly from the OCM.

3.1.2 Supplier Listing (Approved Unauthorized Suppliers)

3.1.2.1 The approved unauthorized supplier should maintain a listing of sub-tier suppliers. The listing should be maintained by a method that allows identification of dates when sub-tier supplier status was changed (e.g., approved/removed, or reclassified within the listing). The sub-tier supplier listing should have at least five different confidence levels defined which enable the selection of the lowest-risk sub-tier suppliers whenever possible. As an example, these levels could be defined as follows:

a. Authorized. The sub-tier supplier is contractually authorized by the OCM to buy parts directly from the OCM and sell parts to customers with full product traceability and warranty.

b. Preferred. The unauthorized sub-tier supplier has been fully assessed per Section 3.1.3 and passed the recommendations of this document and any other requirements. The sub-tier supplier has been used for at least ten purchases of electronic parts by the approved unauthorized supplier with no suspect or confirmed counterfeit, or major nonconforming parts detected. There are no outstanding unresolved quality or delivery issues.

c. Acceptable. The unauthorized sub-tier supplier has been fully assessed per Section 3.1.3 and passed the recommendations of this document and any other requirements. The sub-tier supplier has not yet been used for at least ten purchases, but has had at least two purchases. There have been no suspect or confirmed counterfeit or major nonconforming parts detected. There are no outstanding unresolved quality or delivery issues.

d. Probationary. The sub-tier supplier has not been used for at least two total purchases, or was previously listed Authorized, Acceptable, or Preferred, and was downgraded due to significant quality or delivery issues identified by the approved supplier, GIDEP or other industry databases, that have since been resolved. The sub-tier supplier may regain Acceptable, Preferred, or Authorized status after a minimum of five authentic shipments and resolution of any other issues above, as well as a re-evaluation of the sub-tier supplier in accordance with Section 3.1.3. When a sub-tier supplier has no prior transactions, the sub-tier supplier should be considered Probationary pending full assessment in accordance with Section 3.1.3. A Prohibited sub-tier supplier that has implemented acceptable corrective actions and been re-evaluated in accordance with Section 3.1.3 may be upgraded to this category.

e. Prohibited. The sub-tier supplier has delivered suspect or confirmed counterfeit or major nonconforming parts, or has significant unresolved quality or delivery issues identified by the approved unauthorized supplier, GIDEP, or other industry databases. This includes active suspensions or debarments indicated in the System for Award Management (SAM), previously known as the Excluded Parties List System (EPLS). A Prohibited sub-tier supplier that has implemented acceptable corrective actions and been re-evaluated in accordance with Section 3.1.3 may be upgraded to Probationary.

3.1.2.2 If an Authorized, Preferred, Acceptable or Probationary sub-tier supplier is determined to have supplied suspect or confirmed counterfeit or major nonconforming parts, the approved unauthorized supplier should request corrective actions and down-grade the sub-tier supplier to Prohibited. The sub-tier supplier should remain Prohibited until corrective actions have resolved all of the approved unauthorized supplier's concerns. If a sub-tier supplier has non-counterfeit issues (such as those described in 3.1.2.1.d), the approved unauthorized supplier may down-grade the sub-tier supplier to either Probationary or Prohibited, depending on the severity of the issues.

3.1.2.3 If a sub-tier supplier is classified Prohibited or removed from the supplier listing for shipment of suspect or confirmed counterfeit parts, the approved unauthorized supplier should review all prior purchases of electronic parts from the suspect sub-tier supplier for the last two years. Approved unauthorized suppliers should determine whether testing was sufficient at the time to detect the reported method of counterfeiting. If the previously purchased parts from the suspect sub-tier supplier and inspection/testing is deemed insufficient, the approved unauthorized supplier should re-authenticate in-house parts. If additional parts are determined to be suspect counterfeit, or if parts are not available for re-authentication, the approved unauthorized supplier should notify all affected customers in writing.

3.1.3 Supplier Assessment

The approved unauthorized supplier should have a documented process for assessing all new or previously approved sub-tier suppliers. The process should identify criteria by which the sub-tier suppliers are deemed not acceptable (e.g., Prohibited). The assessment process below contains important actions to ensure that a sub-tier supplier is not prone to delivering counterfeit electronic parts.

The assessment process should include, but is not limited to, the following items. A recommended periodicity for performing these items is provided. Each contractor purchasing organization should evaluate and define a periodicity based on their specific conditions.

a. Review of GIDEP database for past unresolved quality issues (monthly), to include Alerts, Safe-Alerts, Problem Advisories, and Agency Action Notices.

b. Review of other peer databases for past unresolved quality issues if applicable (monthly).

c. Review of the sub-tier supplier's past history, including quality or delivery problems (every 3 months).

d. Review of Corrective Action Requests (CARs) as necessary to upgrade/downgrade the sub-tier supplier.

e. Trade references (for initial screening).

f. Review of active suspensions and debarments indicated in the System for Award Management (www.sam.gov) (every 3 months).

g. Years in business (for initial screening), indicates stability or whether business has changed names recently.

h. Banking information (for initial screening), indicates financial stability.

i. Memberships in distributor organizations (for information only).

j. Quality Management System (QMS) certifications (every 6 months).

k. Insurance and warranty (every 6 months).

The approved unauthorized supplier should re-evaluate Preferred, Acceptable, or Probationary sub-tier suppliers before purchase if six months have passed since the last purchase of parts from the sub-tier supplier.

3.1.4 Stock Parts

Electronic parts already in stock at the approved unauthorized supplier's facility may be used to fill orders for the contractor purchasing organization. Parts in stock which can be proven (i.e., traceability documentation to the OCM) to have been purchased directly from an authorized supplier in original unopened packaging can be sold as authorized supplier parts and be classified as Authorized Stock. If the parts in stock were not bought directly from an authorized supplier by the approved unauthorized supplier, the parts should be considered unauthorized supplier parts. This includes contractor or government excess parts which the approved unauthorized supplier has bought, unless the parts are in original factory-sealed packaging with full traceability to the OCM. Electronic parts not bought directly from an authorized sub-tier supplier should be classified as either Stock Confident or Stock Unknown. Stock Confident parts that are MIL-Spec parts need to pass all inspections and test requirements of their original part specification (SMD or MIL-Spec slash sheet). Stock Confident parts that are not MIL-Spec parts have to pass the inspections and test recommendations provided in Section 5. Stock Unknown is all remaining product.

Stock parts should be stored in a manner that does not reduce traceability, reliability, and quality of the parts (e.g., mixed or combined shipments). This may include assignment of unique internal part numbers to separate parts of different pedigree.

Returned Parts and Restocking: Parts returned to the approved unauthorized supplier for reasons other than suspect or confirmed counterfeit should be segregated with traceability maintained of the return status. Those returned parts should be classified as Stock Unknown. In order to regain Stock Confident status (revalidate traceability documentation), those returned parts should pass all inspection and test requirements of the original part specification (SMD, MIL-Spec slash sheet), and those in Section 5, as well as confirming the expected lot and date code information.

3.1.5 Priority of Sale

The approved unauthorized supplier should supply electronic parts to the contractor purchasing organization in the order indicated in Table 3-1, with parts available in the Order Priority 1 row supplied first. If parts are available both for purchase from the supply chain and from stock, and the order priority is identical, the approved unauthorized supplier may choose from where to supply the parts.

Table 3-1. Order of Purchase, by Supplier or Stock Classification Status

Order Priority	Sub-tier Supplier Classification Status (Purchase)	Stock Classification Status (In Stock)
1	Authorized	Authorized Stock
2	Preferred	Stock Confident
3	Acceptable	Stock Unknown
4	Probationary	

For example, if parts are available from a Preferred sub-tier supplier and are also available as Stock Confident parts in the approved unauthorized supplier's warehouse, either or both sources can be used

to supply parts. If, however, Authorized parts are available either through purchase by the approved unauthorized supplier or in stock, those parts should be first priority.

Stock Confident parts can be provided without additional inspection and test, provided all additional customer-specific requirements have been met. The compliance report should be provided with the shipment. Stock Unknown parts should pass the inspection and test requirements of Section 5 or applicable industry standards such as AS5553, and be upgraded to Stock Confident before the parts can be provided, with the corresponding report.

The approved unauthorized supplier should notify the contractor in writing (e-mail is acceptable) if either of the following conditions is a necessary requirement to fulfill the sale:

a. The order of preference specified in Table 3-1 will not be followed (e.g., Stock Confident is quoted instead of Authorized).
b. The sub-tier supplier will be Probationary or Prohibited.
c. The contractor requires notification if sources or stock other than Authorized are used.

3.1.6 Validation of Parts

All parts purchased by the approved unauthorized supplier that are not provided to the contractor as Authorized (i.e., purchased directly from an authorized supplier) should undergo the inspection and test recommendations of the original part specification (SMD, MIL-Spec slash sheet), and those in Section 5.

All parts purchased by the approved supplier that are not provided to the contractor as Authorized (i.e., purchased directly from an authorized supplier) should have Objective Quality Evidence (OQE) verification as identified below:

a. The part traceability should be verified from (1) traceability documentation or (2) authentication verification (e.g., identification through secure physical markings or unique surface characteristics), or
b. Inspection and testing should undergo the inspection and test recommendations of the original part specification (SMD, MIL-Spec slash sheet), and those in Section 5.

3.2 Approved Supplier Obligations

The approved (authorized and unauthorized) supplier should be responsible to comply with all the recommendations of this section. In addition, the approved supplier should:

a. Meet all contractual specifications and requirements (exceptions or waivers are not allowed unless provided in writing by the contractor).
b. Maintain records and documents as indicated in this document, and make them available for examination during surveys or audits.
c. Permit the contractor to conduct site surveys and audits.
d. Document and maintain a corrective/preventive action program to achieve positive results and continuous improvement.
e. Document and maintain a process for acceptance of returns that ensures returned non-suspect parts are segregated with return documentation, and parts are revalidated.

f. Document and maintain a process for acceptance of returns that ensures returned nonconforming or suspect/confirmed counterfeit parts are segregated in a controlled area for further analysis and disposition.

g. Flow down applicable contractual requirements to all direct sub-tier suppliers and external testing facilities.

h. Be accountable and responsible for the performance of their sub-tier suppliers and external testing facilities.

i. Notify the contractor of major changes in the supplier's QMS, processes, process controls, personnel, points of contact, equipment, or facility locations prior to implementation.

All exceptions to the recommendations above should be approved by the contractor (customer).

3.3 Approved Supplier Evaluation

3.3.1 Factors to Consider

An evaluation of the approved unauthorized supplier should be performed by the contractor, and should include consideration of the following factors:

a. Contract history,

b. QMS certifications,

c. Past performance data (e.g., quality or delivery problems and GIDEP). For government agencies sources such as Product Deficiency Reporting and Evaluation Program (PDREP), Joint Deficiency Reporting System (JDRS) including DoD reports, CARs, and supplier audit reports should be considered.

d. Data from other sources (e.g., supplier audits, Federal Aviation Administration (FAA) supplier information, NASA database, Nadcap audits, or other independent assessments),

e. Suspensions, exclusions, and debarments as indicated in SAM or other government listings,

f. Compliance to all other recommendations of this document, and

g. Validation of inspection and test capability (internal or through the use of third-party facilities), and

h. Insurance and warranty.

3.3.2 Inspection and Test Capability

Validation of inspection and test capability should be accomplished by confirmation that:

a. Facility has passed the DLA laboratory suitability audit for MIL-STD-202, -750 and/or -883, or

b. Facility is certified to an accepted certification standard and the certifications acceptable to the contractor and the approved supplier, or

c. Facility has acceptably complied with all recommendation of this document and any additional contractor requirements.

3.4 Site Surveys (Audits)

Prior to approving a supplier the contractor should require and perform a site survey (audit) of the approved supplier's facility, including any outsourced test facilities. Surveys should include a review of the QMS and all of the systems and processes that the approved supplier has in place and in use, under this document, and all OCM agreements for parts and product lines for which the approved supplier claims to be authorized, including warranty support and OCM product ownership. The purpose of the audit is to ensure that the approved supplier has in place and in daily use processes which conform to this document.

Industry or other third-party surveys or audits may be considered by the contractor in addition to, or in lieu of, site-survey requirements.

3.5 Removal/Disapproval Justification

Continued status as an approved supplier is contingent upon continuing compliance with the criteria and provisions upon which approval is established. Failure to comply will be cause for removal/ disapproval of the supplier. Examples of reasons for removal/disapproval include, but are not limited to the following:

a. Failure to comply with the priority of sale requirements which direct purchases from authorized suppliers as a first priority.

b. Failure to perform and document all applicable inspections and tests.

c. Reporting parts as purchased directly from an authorized sub-tier supplier, but failing to prove that via traceability documentation.

d. Failure to report suspect or confirmed counterfeit parts to the contractor and GIDEP.

e. Failure to prevent suspect or confirmed counterfeit parts from reentering the supply chain.

f. Failure to disclose the sub-tier supplier, or providing an incorrect sub-tier supplier name.

g. Denial of facility access to the contractor.

h. Debarment.

i. Available information has shown repeated poor quality track record with valid complaints.

j. Failure of an audit.

3.6 Renewing Approval

3.6.1 Periodic Approval

Approval is recommended to be performed at least every two years by the contractor.

3.6.2 Approval After Removal/Disapproval

If a supplier has been removed or unapproved, re-approval should not occur until the contractor has determined that all noted deficiencies, concerns, or corrective action requests have been corrected. The supplier should document, to the contractor's satisfaction, the deficiencies or concerns that have been corrected and the implementation dates. Any revisions or additions to the Quality Manual since the removal or disapproval should be documented in the application.

4. Mechanisms to Enable Traceability of Parts to Suppliers

DFARS rule, 48 CFR 252.246-7007(c)(4) requires the establishment of "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. This traceability process shall include certification and traceability documentation developed by manufacturers in accordance with government and industry standards; 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 part(s), such as date codes, lot codes, or serial numbers. If IUID marking is selected as a traceability mechanism, its usage shall comply with the item marking requirements of 252.211-7003, Item Unique Identification and Valuation."

This section establishes a recommended approach for requirements, polices, and activities for managing and implementations for electronic part traceability when buying from an unauthorized supplier.

4.1 Certification of Conformance for Traceability

4.1.1 Part Traceability

The unauthorized supplier should provide traceability documentation from the OCM to the unauthorized supplier; including all intermediaries who have had custody of these electronic parts. The traceability documentation should include, at a minimum, (1) the CoC, which includes the name and location of all of the supply chain intermediaries from the part manufacturer, (2) the device number, and (3) the lot number and/or date code to the direct source of the product to the seller. There may be multiple CoCs.

The contractor should review and validate traceability documentation. This includes verifying the part number against the purchase order and the marking on the packaging. Verify CoCs against flow down requirements for accuracies such as misspelled wording, supplier address, quantity listed against purchase order, and signature of the quality assurance official. See Figures 4-1 and 4-2 for examples of good and bad CoCs.

In the event that sufficient traceability data is not obtained and satisfactory traceability cannot be confirmed, then the testing and inspections defined in Section 5 should be implemented.

4.1.2 Reverse Traceability

Reverse traceability is the capability of the OEM to determine the original source of the part once it has been installed into the end item hardware. For most NSS programs, the contractors have a requirement to be able to reverse trace parts installed in flight hardware. They are required to provide the information when requested by the government program office or deliver (as a Contract Data Requirements List (CDRL)) an As-Built, Parts, Materials and Processes List (ABPMPL). The specific requirements of the AMPMPL can be found in TOR-2006(8583)-5235. This capability allows both the contractors and the government program offices to determine if their already built hardware is affect by a GIDEP or other industry alert. The advantage of the ABPMPL is knowing what was built into your system and the ability to perform risk assessments and cost estimates when issues arise when the hardware is installed into the end item system.

Certification of Conformance

Ω±µ Advanced Technologies Group Inc. Ω±µ

A Distributor of Electronics Components

6452 EEE Way

Lincoln, NE 68501

Shipped From	Assembled In	
N/A	N/A	6000 Component Way, Richmond, VA 23218
N/A	XXX	4525 Electrical Street Seattle, WA 98101

Sold To: Acme Space Systems — **Date Shipped 1/15/2014**

Purchase Order Number: 09MLK00061 — **QTY Shipped: 1500**

Customer Part Number: 2354698-187 — **Customer Rev: C**

MFR Part Number: JANS2N2241A — **MFR Rev. B**

Date Code: 1338 — **Lot Number: 96**

Manufactured By: UNLIMITED IC's CO.

Manufacture Address: 6845 IC Lane, New York, NY, 10007

Under the authority vested in my origination, it is herby certified that the material described above were derived from a lot of material certificated by the manufacture to conform to the applicable requirements of the specification listed. Physical, Electrical, and/or chemical test reports are on file with us or our suppliers indicated conformance with applicable specification review. The seller has been duly authorized to handle and distribute the items furnished and has processed the specification. Any semiconductors in this shipment have been protected from ESD damage in accordance with the methods outlined in JESD625 during storage and handling and shipment from this facility.

Signature/ Title	Date	
John E. Henry/ QA Manager	1/14/2014	

Figure 4-1. Example 1: Good CoC

Figure 4-2. Example 2: Bad CoC

5. Inspection and Testing of Electronic Parts, Including Criteria for Acceptance and Rejection

DFARS rule, 48 CFR 252.246-7007(c)(2) requires the inspection and testing of electronic parts including the establishment of acceptance and rejection criteria when procuring from other than authorized suppliers. “Tests and inspections shall be performed in accordance with accepted government- and industry-recognized techniques. Selection of tests and inspections shall be based on minimizing risk to the government. Determination of risk shall be based on the assessed probability of receiving a counterfeit electronic part; the probability that the inspection or test selected will detect a counterfeit electronic part; and the potential negative consequences of a counterfeit electronic part being installed (e.g., human safety, mission success) where such consequences are made known to the contractor.”

Per DFARS rule, 48 CFR 252.246-7007(c)(7), “methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit” are required.

When electronic parts are procured from an unauthorized supplier the following steps are recommended to reduce the risk of obtaining counterfeit parts.

The minimum number of tests and inspections recommended are listed in Section 5.1 and described in its subparagraphs. Any discrepancy resulting from the testing/inspection below should be dispositioned by the using entity. For additional tests and inspections, refer to MIL-STD-750, -883 and -1580.

5.1 Inspection and Test

The contractor purchasing organization should ensure that appropriate inspection and testing is performed for all part shipments that were not bought directly from an authorized supplier with full traceability documentation. The testing facility should be assessed and accepted by the customer/ contractor. The contractor should determine who will do this testing and where this testing will be performed. The following tests are recommended and have been found valuable in detecting counterfeit parts:

a. Certificate of Conformance (CoC)
b. Complete history of the part
c. Handling history
d. Pictures
e. Part marking and Lot Date Code (LDC)
f. Visual inspection
g. Marking and surface finishing tests
h. X-Ray
i. X-Ray Fluorescence (XRF)
j. Decapsulation / Die Verification
k. 100% electrical testing (room, hot, cold) and Statistical Process Control (SPC)
l. Seal testing, where applicable based on part type
m. Additional tests as required by the customer

5.1.1 Traceability Documentation

Reference Section 4 for additional guidance on traceability. Documentation should be provided by a supplier formally declaring that all customer purchase order requirements have been met. Examples of traceability documentation are:

a. Name, address, and phone number of the authorized supplier

b. Statement that the supplier is not an authorized supplier, when applicable

c. Contractor purchase order number

d. Part number

e. Part manufacturer (OCM)

   When available, the CoC from the OCM should be authenticated with the OCM to reduce the risk of counterfeit parts. It should also be noted that the presence of a CoC does not guarantee the parts are authentic.

f. Lot code

g. Date code

h. Quantity

i. Name and address of the company that the electronic parts were acquired from and any CoC available pertaining to the supply chain custody of the part acquired

j. Name and address of the company performing any or all of the baseline inspections and tests

k. Date that inspections and tests were completed

l. Certification that all parts inspected passed all authenticity inspections and tests

m. Signatures of supplier's Quality Assurance (QA) manager and inspector

5.1.2 Handling History

Section 5.1.1 discussed the paperwork trail requirements. In addition, each facility that has possession of the electronic parts should physically handle the parts appropriately. The preferred storage of the electronic parts should be in the OCM electrostatic discharge (ESD) packaging and all handling should be at ESD approved work stations by ESD protected personnel. A record of all handling should be kept in ESD approved bags with the electronic parts. If additional testing is required, a record of the tests that were performed and the results should also be kept with the electronic parts.

5.1.3 Images

The purchasing party should request hi-resolution photos of the parts, including top and bottom of the package, as well as the side view of the leads, so that all part markings are clearly visible and lead configuration can be verified. Photos should be examined for evidence of surface sanding to remove original part markings, font, and layout of existing part marking and OCM logo. This information should be verified with the OCM or images of known authentic devices for authenticity. Photos or scanned copies of all paperwork should also be reviewed by the purchasing party. If available, the photos should be sent to the procuring activity prior to placing the purchase order.

5.1.4 Part Marking and Lot Date Code (LDC)

If possible, verify part marking with the OCM. All data gathered in Sections 5.1.2, 5.1.3, and 5.1.4 should be forwarded to the OCM for verification. The OCM should validate that the photo of the part appears to have authentic part marking, the CoC was issued by them and that they manufactured this type of electronic part with this LDC. If the OCM no longer exists due to obsolescence, then the data should be compared to a previous purchase order received directly from them by the customer/contractor. Verify the lot date code is consistent with the production timeline.

5.1.5 Visual Inspection

An incoming enhanced visual inspection is required to validate that the parts received match the requirements of the parts ordered. Visual inspection should be performed on a 100% basis. The associated paperwork should also be inspected to validate that it matches the parts.

5.1.5.1 External Package Inspection

All samples should be measured to verify proper package dimensions and lead spacing. There should be no variation or discrepancy within the lot. The lead finish should be verified with the part requirement. The leads including the side view should be inspected at 30x minimum for evidence of re-lead forming, flaking metal finish, or corrosion. The part marking surfaces should be inspected for evidence of sanding, etching, or scraping with an abrasive tool. If no sanding or scraping is evident, the surface should be inspected at 30x minimum with bright white light for evidence of residual ink from previous marking. Parts should be inspected for other evidence of counterfeiting in accordance with industry standards (e.g., AS5553).

5.1.5.2 Documentation Inspection

All paperwork should be inspected for consistency and should match the parts purchased. If the OCM CoC is available, it should be reviewed by the OCM to validate its authenticity. All available screening and qualification data should be per the applicable MIL-Spec and should be validated for authenticity by the OCM.

5.1.5.3 Part Marking Inspection

A resistance to solvents test per Table 5-1 should be performed on the part marking per MIL-STD-883, Method 2015. The manufacturer's logo, the font, and the general marking layout should be compared to a known good part. Digital pictures can be sent to the OCM to verify authenticity.

5.1.6 X-Ray

Real time X-ray should be performed per the applicable part specification on a 100% basis. Any discrepancy (e.g., inconsistent or incorrect internal construction) within the package is rejectable. Criteria for X-ray inspection should be per the applicable MIL-Spec for that part type. If the part number has been purchased previously from the same OCM, and radiological images were stored, the prior images should be compared to the new images for this authentication effort.

5.1.7 X-Ray Fluorescence (XRF)

XRF should be performed on a sample of three (3) to verify plating finish and that no prohibited materials are present. This test may be omitted if this verification is performed by another test [e.g., Energy Dispersive X-Ray (EDX) during Destructive Physical Analysis (DPA)].

5.1.8 Marking and Surface Finishing Tests

The inspection/test facility should perform the following testing on the parts to determine if the part surface has been sanded, resurfaced, or remarked. Inspection should check for the removal of ink markings or surface coatings. The results should be documented to the minimum requirements of Table 5-1, and should include any noncompliance.

Table 5-1. Marking and Surface Finishing Test Requirements (as applicable)

ID	Further Detail[1,3]	Destructive[4]	Sample Size[5,6]	Pass Criteria	Supporting Information[2]
3A	Resistance to Solvents	Yes	3	No removal of ink markings or surface coatings, per applicable MIL-Specs for each device type.	Provide images of worst case part, before and after, with used cotton swab.
3B	Remaining Inspection (Aggressive Chemical Test)	Yes		No removal of coating per AS6081.	Provide images of worst case part, before and after, with used cotton swab.
3C	Scrape test	Yes	3	No flaking or peeling of surface.	Provide images of worst case part, before and after scrape.
3D	High Magnification (SEM or up to 200X optical microscope) Visual	No for optical microscope Yes for SEM	3	No removal of surface coatings.	Provide images of worst case part before and after.

Notes:

1) Samples should be taken from random locations within the shipment.
2) Images should be provided in color at a resolution of at least 5 megapixels.
3) For all solvents, ensure proper safety precautions are used, including proper Personal Protective Equipment (PPE), a ventilated fume hood, and eliminate any ignition sources.
4) Parts which undergo destructive tests should not be considered acceptable for flight. Parts used for non-destructive test (test 3D) may be used for one of the destructive tests after completion.
5) For small lot sizes, less than ten (10) devices, this “destruct” test sample size may be reduced to one (1) device at the discretion of the Cognizant Engineer with Quality Assurance concurrence and Customer approval.
6) Sample sizes derived from AS6081

3A. Resistance to Solvents Inspection

Perform this inspection on the agreed upon sample size per the applicable MIL-Specs. This inspection should be performed on ink and other markings susceptible to solvents (not applicable to markings such as molded, laser. or embossed). If this inspection is not performed due to the marking type, the test report should indicate why the inspection was not performed.

3B. Remarking Inspection Using Aggressive Chemicals

Perform this inspection on the agreed upon sample size per AS6081. Use 1-Methyl-2-pyrrolidinone and 4-Dynasolve® 711 or 750 (as alternates, Dynasolve® 715 or 760 may be used for this test).

3C. Blacktop Scrape Inspection

Perform this inspection on the sample size indicated in Table 5-1 herein. Lightly scrape the device surface with a sharp blade to see if a coating has been applied to hide original marking re-work. Peeling or flaking material indicates possible blacktopping.

3D. High Magnification (Scanning Electron Microscopy (SEM) or up to 200X Optical Microscope) Visual

Visual inspection should be performed in accordance with the test lab standard. The inspector should identify any of the following:

a. Detection of micro abrasion indicative of original marking removal
b. Detection of abrasive particles indicative of sanding or microblasting
c. Detection of minute surface finish variations indicative of flat lapping

5.1.9 Decapsulation/Delidding (for all parts) / Die Verification (for active parts)

Since DPA per MIL-STD-1580 is required as a normal process of space part verification, the additional verification below should be performed to mitigate the procurement of counterfeit parts. If formal DPA is not required then the additional verification steps below should still be performed. The contractor/ customer should approve the DPA lab and process used.

The inspection/test facilities should decapsulate and examine under magnification (100-500X) a sample of three (3) pieces of each date code per applicable MIL-Spec for part type (i.e., MIL-STD-883 for integrated circuits (IC), MIL-STD-750 for semiconductors, etc.). Prohibited material verification should be performed to ensure no prohibited material exists. Since this test is destructive, all devices subjected to this test should be clearly identified and segregated from all other devices.

Inspect microcircuits, transistors, and diodes (except axial lead hermetic) using MIL-STD-1580.

Inspect axial leaded hermetic diodes and passive parts by cross-section analysis using MIL-STD-1580. Verify that the component characteristics are consistent with the manufacturer's data and/or a known good sample. The device being inspected and the known good sample should be photo documented for later reference.

For active parts: The magnification should be sufficient to identify basic die layout (e.g., capability to detect die differences large enough to detect on a full-die photograph), as well as individual die markings or logos (typically requires at least 300 times magnification). The inspection should look for variations in the die topology, manufacturer's logo, and other die markings. All variations from the known good die should be verified with the manufacturer. The device being inspected should be compared to known good samples or photographs of known good devices. All photographic images should be preserved without altering the original spatial resolution or pixel density. The use of Joint Photographic Experts Group (JPEG) or other 'lossy' file formats is not recommended.

5.1.10 Electrical testing

Electrical testing should be performed in order to validate that the parts meet their advertised datasheet parameters. The parameters tested should be sufficient to verify the key features of the

parts, validate no opens or shorts, and verify the parts meet the specification limits. This is necessary to rule out the parts being electrical rejects from the original production process or mixed with a counterfeit lot. If the unauthorized supplier has all the electrical test data for the lot and the part numbers are serialized, then a randomly selected sample test should be performed at 25°C, as well as the specification high and low temperature per the applicable part specification and/or applicable MIL-Spec. The sample size should be 10% of the lot or 10 piece minimum if the lots size is smaller than 100 pieces. This data should be compared to the OCM's existing data in accordance with calibration testing parameters (i.e., serial # by serial #). If any discrepancy exists or if data is not available or the parts are not serialized, then 100% of the lot should be tested at 25°C, high and low temperature per the applicable specification, including all applicable testing [e.g., Direct Current (DC), Alternating Current (AC), Functional]. In addition, a 3-sigma calculation should be used to determine lot variability. Any failures or variability should be reviewed by the customer prior to accepting the lot to determine if this is common for that part type based on historical data.

Parametric variability or open /short failures may be due to any of the following items:

- Wrong die
- Damaged or stressed or used part
- Production rejects or lower performance parts

If the parts fail to pass the tests listed herein or any other customer-required tests, the unauthorized supplier should notify the customer within 5 working days of the failure, and provide all relevant information (e.g., failing parameter, test limits, and reading). The unauthorized supplier should undertake additional non-destructive inspections or tests (e.g., burn-in with no failures) to determine if the parts are suspect counterfeit. The customer may request sample parts in order to perform an assessment or perform life test on a sample basis per the applicable MIL-Spec. Parts should not be subjected to destructive tests without customer approval. Parts which are determined to be suspect or confirmed counterfeit due to additional (customer required) testing are subject to the Section 6 reporting and quarantining requirements.

5.1.11 Hermeticity

Seal test should be performed on a 100% basis for all hermetically sealed devices per MIL-STD-883/Method 1014 (Krypton 85 leak test) or the applicable specification requirement based on part type to determine that there are no leakers that fail the applicable MIL-Spec requirement. However, if the parts were previously subjected to gross leak tests using fluorocarbons then the Krypton 85 leak test is not required.

5.1.12 Data

Document the results of the above tests in a test report. Test data should be reviewed by the contractor's cognizant specialty engineer for the part type. If there are any discrepancies or potential of a suspect part, then the parts need to be locked down. The cognizant specialty engineer and the contractor's legal team need to disposition the anomalies. If the anomalies indicate any suspect counterfeit, then the entire lot needs to be quarantined and handled per Section 6.

5.1.13 Test Lab Certification

All test labs should be certified and approved by the customer prior to use and/or be certified by a DLA laboratory suitability audit. Certification should include, at a minimum, an audit of the test facility to validate the part handling procedures, test equipment and operating procedures, and the

calibration status of all equipment. A responsible test lab (RTL) should be able to meet the following criteria.

An RTL, to whom parts are sent by the User/Requester to perform the complete (or agreed upon) suite of tests for suspect/counterfeit parts inspection, acts as the sole point of contact for the User/Requester for matters concerning the execution of those tests, including managing the overall test sequence and completing the formal test report or supplying any requested data. The RTL should be per ISO/IEC 17025 accredited or be able to meet the requirements of ISO/IEC 17025. The RTL should communicate with the User/Requester to verify the Test Requirements as specified in the SOW, including the tier level of risk associated with the parts (if provided). The RTL can be either an in-house (same organization as the User) Test Laboratory or an outside test facility.

5.1.13.1 Test Laboratory/Test Facility

The Test Laboratory/Test Facility should have documented procedures under revision control and have the proper equipment, capabilities, and personnel in place to conduct the counterfeit parts inspection herein that it contracts to perform, including the following:

1. Meet Occupational Safety and Health Administration's (OSHA's) regulations that pertain to a Test Laboratory Facility.
2. Have the proper test equipment, fixtures, support/calibration/standardization equipment, test material, and reference standards defined in the specific procedures.
3. Subcontracting of Test Methods should only be performed by the RTL. If any inspections are to be subcontracted by the RTL, the RTL should notify and obtain written approval from the User/Customer of its intent to subcontract, prior to the initiation of testing.
4. Sufficient technical personnel should be employed by the Test Laboratory, with the proper credentials.

The Test Laboratory should be able to demonstrate proficiency in those inspection and testing methods for detecting counterfeit electronic parts by being able to identify known counterfeit parts.

The Test Laboratory seeking to demonstrate proficiency for the specific inspection should establish an auditable method and a process to validate that the Test Lab is able to meet the provisions of the specific proficiency requirements. The Test Lab demonstrates its competency though key comparisons, inter-laboratory comparisons, or proficiency tests appropriate to validate their testing capability. The process and methodology selected by the Test Lab should include the following:

1. Demonstrate that the required training is obtained by the personnel and is periodically refreshed.
2. Be able to detect counterfeit parts using the specific inspection technique.
3. The equipment chosen to do the work should be able to meet the accuracy, resolution, and repeatability required.
4. The laboratory should either have had its competency independently assessed through the process of laboratory accreditation or performed a complete self-assessment.
5. The specific inspection process should be documented in the form of a written procedure.

Examples of specific proficiency requirements for the specific counterfeit parts inspection process should be documented in the individual inspection procedures specified herein.

5.1.13.2 Calibration

The Test Laboratory should have an established Calibration Policy and Procedure that is documented and under revision control, with the following characteristics:

1. Control measurement processes to ensure the accuracy of measurement results affecting all Test Methods specified herein.
2. Establish and maintain traceability of measurement results by an unbroken chain of calibrations through the National Institute of Standards and Technology (NIST), or an institution recognized by NIST through international agreements, to the International System of Units (SI) when such units have been established.
3. Control the accuracy, reliability, and use of Measuring and Test Equipment (MTE) through the use of a calibration system compliant with the requirements of American National Standards Institute/National Conference of Standards Laboratories (ANSI/NCSL) Z540.3-2006 and applicable requirements of Society of Automotive Engineers (SAE) AS9100, subject to the clarifications and modifications provided in the detailed counterfeit parts inspection procedures specified herein.

Examples of specific calibration requirements for the individual counterfeit parts inspection procedures should be as documented herein.

5.1.13.3 Device Handling Requirements

The Test Laboratory should have an established Device Handling Policy that is documented and under revision control, and should include ESD, moisture, and radiological precautions and handling requirements either as part of the procedure or referenced as a separate procedure under revision control. If the Test Laboratory has test equipment that emits radiation, the Test Laboratory should have a Radiation Sensitive device handling policy in place that is part of or referenced by the laboratories Device Handling Policy for radiation sensitive devices.

The following general precautions should be observed in device handling:

1. Devices should not be subjected to conditions in which voltage or current transients cause the maximum ratings to be exceeded.
2. Precautions should be observed in testing microelectronic devices in radiographic fields of energy, not to exceed specified dose levels.
3. For microelectronic device handling, ground all equipment prior to insertion of the device for electrical test. Keep devices in metal shields, or equivalent until they are inserted in equipment to test. Where applicable, keep devices in carriers or other protective packages during test.
4. Provide for interim storage of parts before, during, or after test, as required.

5.1.13.4 ESD Sensitive Devices

The Test Laboratory should have a documented internal process and procedure to handle ESD sensitive devices. The requirements of either ANSI/ESD S20.20 or Joint Electronics Device Engineering Council (JEDEC) STD JESD625 should be followed in handling ESD sensitive devices.

5.1.13.5 Moisture Sensitive Devices

The Test Laboratory's Device Handling Policy should include handling procedures in accordance with JEDEC Standard J-STD-033 or equivalent for moisture sensitive devices. The Test Laboratory should be notified by the User Organization of the Moisture Sensitivity Level (MSL) of the devices, if applicable, as part of the Statement of Work (SOW).

5.1.13.6 Radiation Sensitive Devices

The Test Laboratory should have a Radiation Sensitive device handling policy in place that is part of or referenced by the laboratory's Device Handling Policy for radiation sensitive devices.

5.1.13.7 Sampling Procedure

The Test Laboratory should generate a Test Sequence document or traveler, to complement the counterfeit part inspection test plan supplied by the User Organization.

The Test Sequence document should as a minimum delineate or outline the following:

1. Pertinent User Information and device lot Information, including name of user and address, device type, quantity and nomenclature, original device container(tape/reel), lot size, date/lot code, location of device manufacture, etc.
2. The specific counterfeit parts scheduled inspections to be performed (e.g., radiographic, electrical) and the quantity to be inspected.
3. Document the specific procedure on how the samples were selected for inspection, either randomly from beginning, center, or end of reel, or on devices showing anomalous variations from the mean of the lot.
4. The procedure for removing samples from the initial container, handling, inspection and labeling the test samples, and protecting devices while waiting for specific inspections, and repackaging samples following inspections. This should include specific handling, labeling, and packaging of moisture and ESD sensitive devices. The handling and storage procedures should be maintained from receipt of parts through inspections, storage, test, protective repackaging and shipment back to the User Organization.
5. Procedures and packaging for protection of component leads/solder balls from damage.
6. Transportation packaging, equipment, and methods to prevent packages from being dropped or dislodged during shipping.

5.1.13.8 Temperature and Relative Humidity

The Device Handling and Test Inspection Area Temperature and Relative Humidity should be controlled and documented during the period of time that the Test Laboratory receives, inspects, and sends back the test lot of devices to the User/Requester in accordance with ANSI/ESD S20.20 or JEDEC STD JESD 625. In areas of low relative humidity, follow the requirements specified in ANSI/ESD S20.20 Ionization Standard, S3.1. For guidance on areas of low relative humidity, refer to Appendix B herein.

6. Reporting and Quarantining of Counterfeit Electronic Parts and Suspect Counterfeit Parts

DFARS rule, 48 CFR 252.246-7007(c)(6) requires "Reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts. Reporting is required to the contracting officer and to the Government-Industry Data Exchange Program (GIDEP) when the contractor becomes aware of, or has reason to suspect that, any electronic part or end item, component, part, or assembly containing electronic parts purchased by the DOD, or purchased by a contractor for delivery to, or on behalf of, the DOD, contains counterfeit electronic parts or suspect counterfeit electronic parts. Counterfeit electronic parts and suspect counterfeit electronic parts shall not be returned to the seller or otherwise returned to the supply chain until such time that the parts are determined to be authentic."

In addition to the DFARS requirements companies should also ensure awareness and compliance with reporting to the Office of the Inspector General of the agency, field command, or other component of the DOD for their respective customer as prescribed under Federal Acquisition Regulation (FAR) 3.10.[16]

This section provides suggested implementation details and benefits of Reporting and Quarantining suspect and confirmed counterfeit items. Contractor policies to address Reporting and Quarantining of Counterfeit and Suspect Counterfeit Electronic Parts are a required element of the FY2012 NDAA[17] and DFARS 252.246-7007 (as stated above).

Companies should be mindful that FAR Case 2013-002 "Expanding Reporting of Nonconforming Supplier" which is currently in development at the time of this publication may provide additional regulatory requirements for reporting when published.

6.1 Reporting

The fundamental objective of reporting is to minimize the impact and maximize the containment of the counterfeit item event throughout industry.

Reporting is intended to notify stakeholders and interested parties of findings which may impact their operations or products. Incident reports should be factual and to the maximum extent possible provide actionable information in a timely manner under the protection from civil liability for such disclosures.

When additional or more stringent reporting and/or quarantining of counterfeit and suspect counterfeit items is part of a contractual requirement, compliance with contract requirements takes precedence over guidance provided here.

For the purposes of this document the reporting discussion is broken into four fundamental steps. Each step may require differing levels of coordination or review based on company specific policy. Two of the four steps, Reporting Within the Company and Reporting to Customers, are topics

[16]FAR 52.203-13, Contractor Business Ethics Compliance Program and Disclosure Requirements
[17]H.R.1540 National Defense Authorization Act for Fiscal Year 2012, Section 818, Detection and Avoidance of Counterfeit Electronic Parts (c), (4) & (e) (2) (a) (vi)

addressed as part of an International Standards Organization (ISO) 9001:2008[18] or AS9100C[19] quality management system.

The third and fourth steps, Reporting to Industry and Reporting External to the Company, may represent requirements beyond the quality management system standards. In any case reporting practices specific to counterfeit should be included in the company's counterfeit item detection and avoidance process.

6.1.1 Reporting within the Company

Reporting internal to the company may be accomplished by various means. Companies generally require less oversight and review for internal reporting compared to information released to external sources therefore providing the opportunity to communicate pertinent facts quickly throughout the company.

Companies may find it beneficial to execute internal reporting in steps or phases providing a "heads up" upon initial indication of a suspect counterfeit with updates as the investigation progresses and final conclusions and actions are defined, using protective markings the company may require for such internal disclosures.

Internal reporting should be directed to appropriate resources to ensure effective containment.

Companies should include the following information as part of the internal reporting process:

- Part number of suspect/counterfeit item
- Manufacturer, Date Code, Lot Code, and other identifiers specific to the suspect/counterfeit item
- Nomenclature/Description of the suspect/counterfeit item
- Source and procurement information of the suspect/counterfeit item
- Evidence/how has the suspect/counterfeit item been detected
- Where used information

6.1.2 Reporting Databases

Companies should include review of reporting databases in their counterfeit avoidance policy and procedures. Information from reporting databases can be used as part of supplier and component risk assessment process. There is a variety of government and industry managed databases available for use.

6.1.2.1 SMC and NRO Programs

For contractors working on United States Air Force Space and Missiles System Center (USAF/SMC) and the NRO programs, the Parts, Units, Materials, Processes and Systems (PUMPS) tool should be used to report suspect/confirmed counterfeit incidents. The tool establishes a repository of quality, supplier, manufacturing, testing, and workmanship issues and failures that occur on SMC and NRO

[18]ISO-9001:2008, Quality Management System Requirements, Paragraph 5.5.3, and Paragraph 7.2.3
[19]AS9100C, Quality Management Systems - Requirements for Aviation, Space and Defense Organizations, Paragraph 5.5.3, and Paragraph 7.2.3

programs. Each program enters their information into the tool. The user can upload PowerPoint, word, PDF, etc. files into the tool that provides the background information about the issue. The tool alerts/notifies each program of the issue. Then each program is to respond if they are affected or not affected by this issue.

Some SMC and NRO contractors have been granted limited access to the PUMPS tool. Their access allows the contractors to upload their issues into the tool. Therefore, if the contractor has a suspect or confirmed counterfeit part to report, after notifying the contracting officer, they should upload the report into the PUMPS tool. The PUMPS administrator can then use the contactor information to alert the other programs to the counterfeit item.

6.1.2.2 GIDEP

Department of Defense Instruction (DoDI) 4140.67[20] and the Aerospace Industries Association (AIA) support the use of the GIDEP for reporting of suspect/counterfeit incidents. DFARS 252.246-7007 requires that companies use GIDEP as one of the primary places to report counterfeit incidents.

The GIDEP program is managed by the US government and is a tool for government and industry organizations to issue and access alerts of various types and subject matter including nonconforming and counterfeit parts. Access to GIDEP reports is limited to organizations in the United States and Canada. U.S. or Canadian companies that directly or indirectly conduct business with the U.S. government or support the U.S. government's acquisition of systems, facilities and materiel, may voluntarily participate in GIDEP. See the GIDEP Manual Chapter 2, paragraph 2.2. Additional information regarding GIDEP membership, participation guidelines, and requirements may be obtained at www.gidep.org.

Other customer or industry specific databases may also be useful for counterfeit incident reporting and risk assessment. For example, NASA's Supplier Assessment System contains, in addition to GIDEP data, seizure data from U.S. Customs and Border Patrol. Organizations such as the FAA, MDA, the Space Quality Improvement Council (SQIC), and Department of Energy (DOE) also have reporting and alert processes which should be considered.

In addition to U.S. government managed reporting databases there are private industry reporting databases that focus on counterfeit incident reporting. Companies should consider use of industry reporting databases as a supplement to GIDEP membership or for use when companies are not eligible for GIDEP membership.

6.1.3 Reporting External to the Company

As referenced above, DFARS 252.246-7007(c)(6)[21] clearly states the requirement to report suspect counterfeit and counterfeit items:

> "…to the Contracting Officer and to the GIDEP when the contractor becomes aware of, or has reason to suspect that, any electronic part or end item, component, part, or assembly containing electronic parts purchased by the DOD, or purchased by a contractor for delivery to, or on behalf of, the DOD, contains counterfeit electronic parts or suspect counterfeit electronic parts."

[20] DoDI 4140.67, DOD Counterfeit Prevention Policy, April 26,2013, (4), (j), (1)
[21] See http://www.acq.osd.mil/dpap/dars/dfars/html/current/252246.htm#252.246-7007

Companies should implement processes which enable timely reporting (i.e., within 60 days after the company becomes aware) to help minimize potential impacts throughout the customer and industry community.

Various customers and government agencies may provide agency, program, or contract specific reporting requirements which companies should address in concert with the current regulatory requirements, including mandatory reporting under FAR 3.10, Contractor Code of Business Ethic and Conduct, when applicable. When conflicts are identified companies should engage their contracts and legal counsel to resolve the conflicting requirements with their customer.

In March of 2011 the AIA published a Special Report titled "Counterfeit Parts: Increasing Awareness and Developing Countermeasures"[22]. The AIA report includes information regarding a survey conducted by AIA of the benefits of GIDEP membership and reporting of counterfeits as well as potential obstacles to reporting counterfeit incidents via GIDEP. As mentioned above, companies should also be aware the FY2012 NDAA Section 818[23] includes safe harbor language regarding protecting companies civil liability (e.g., defamation claims) for reporting on "suspect" counterfeit parts. Companies should consult legal counsel and review their policies to ensure compliance with FY2012 NDAA Section 818.

The US DOD Inspector General has published information addressing the FY2012 NDAA Section 818 requirement to report suspect counterfeit item to the government.[24] The Office of Inspector General states "Contractors should report through submission of a contract disclosure." Contract disclosure is further defined as the FAR Clause 52.203-13[25], Contractor Business Ethics Compliance Program and Disclosure Requirements, as proscribed in FAR 3.10. Companies should consult legal counsel to ensure policies and practices are in compliance with regulatory and contractual requirements.

Companies should consult legal counsel for guidance regarding reporting outside of the company.

6.1.3.1 Reporting to Law Enforcement

Companies (contractors) play an important role in enforcement because they are often in the best position to detect counterfeit electronic parts, safeguard important proof, and quickly report a counterfeit. In a digital world where evidence can disappear at the click of a mouse, swift investigation is often essential to successfully prosecute a counterfeit case. Reporting counterfeit electronic parts to law enforcement helps agents develop and pursue criminal cases, ensuring that counterfeiters are brought to justice. Without such referrals, counterfeiters will continue to reap profits from their crimes without fear of punishment, hurting victims, and damaging the interests of the United States. It is vital that companies properly secure evidence of crime so that investigators can be certain of the integrity of that proof and be able to follow accurate leads. Finally, communicating early with law enforcement authorities after discovering a counterfeit will allow a company to coordinate contractual, administrative, or civil proceedings with possible criminal enforcement.

---

[22]Aerospace Industries Association Counterfeit Parts: Increasing Awareness and Developing Countermeasures, March 2011 (http://www.aia-aerospace.org/assets/counterfeit-web11.pdf)
[23]H.R.1540 National Defense Authorization Act for FY2012, Section 818, Detection and Avoidance of Counterfeit Electronic Parts (c), (5)
[24]United States Department of Defense Office of Inspector General, Contract Disclosure Program (http://www.dodig.mil/programs/cd/)
[25]See http://www.acquisition.gov/far/html/52_200_206.html#wp1141983

Whether to Report

Companies use their own criteria and procedures, such as those described in this document, to determine if a received electronic part is a suspect counterfeit part. A company's determination of whether a case should be reported to law enforcement will depend upon that company's judgment and upon the unique facts and circumstances of a particular case. However, when a company becomes aware that it has evidence of a potential crime, it should certainly report the matter to law enforcement. Although individuals or companies can always pursue contractual, administrative, or civil remedies in case of purchase or receipt of counterfeit electronic parts, criminal sanctions may be warranted in appropriate cases to punish and deter wrongful activity. In addition, the company may have evidence that in isolation may seem insignificant, but that may be quite important in the context of a larger investigation into a counterfeiting operation about which the company knows nothing. As a result, companies should generally report counterfeit parts to law enforcement.

Congress has continually expanded and strengthened criminal laws for violations of intellectual property rights (IPR) to protect innovation, keep pace with evolving technology, and—perhaps most importantly—punish and deter persistent and egregious IPR violations. To determine whether to report a counterfeit electronic part to law enforcement requires a basic understanding of federal criminal laws in this area.

For counterfeit items, the most important federal statute is 18 U.S.C. §2320, which covers trafficking in counterfeit goods as well as counterfeit labels. Note that the definition of a counterfeit electronic part may be different under the criminal statutes than it is under other laws and regulations [e.g., DFARS 48 CFR 252.246-7007(a)].

Where to Report

When a company has located a counterfeit electronic part and believes it has evidence of a crime, it should quarantine the item and report the matter to law enforcement in addition to reporting to the contracting officer and the OIG. Although a variety of ways exist to report trafficking of counterfeit electronic parts to law enforcement, a convenient way to report the matter is through the interagency National Intellectual Property Rights Coordination Center (IPR Center) in Arlington, Virginia. Company personnel should go to the link http://www.iprcenter.gov/referral and fill out the online form or, alternatively, email the referral to iprcenter@dhs.gov.

The IPR Center, led by U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI), is a collaborative effort by more than 21 U.S., foreign, and multilateral investigative and regulatory agency partners that work together to combat intellectual property crime. Members include the Federal Bureau of Investigation (FBI), U.S. Customs and Border Protection (CBP), Air Force Office of Special Investigations (AFOSI), Defense Criminal Investigative Service (DCIS), U.S. Army Criminal Investigation Command (Army CID), U.S. Naval Criminal Investigative Service (NCIS), NASA, Defense Logistics Agency (DLA), General Service Administration's Office of the Inspector General, and many others. The IPR Center partners strive to investigate and de-conflict case leads, interdict counterfeit and pirated goods at the borders, and provide extensive training and outreach. The IPR Center also works closely with the Department of Justice through the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS). The IPR Center encourages victims to visit its website at www.iprcenter.gov to obtain more information about the IPR Center.

Steps to Take When Reporting to Law Enforcement

Because companies are generally in a better position than their customers to detect and report counterfeit electronic parts, they play a crucial role in referring possible cases to law enforcement. The Contractor Code of Business Ethics and Conduct (FAR 52.203-13) provides a good starting point for reporting to and cooperating with law enforcement regarding counterfeit electronic parts by all companies, not just contractors. This code states that a contractor's internal control system should provide for, among other things, "[f]ull cooperation with any government agencies responsible for ... investigations....." The code defines "full cooperation" as "disclosure to the government of the information sufficient for law enforcement to identify the nature and extent of the offense and the individuals responsible for the conduct. It includes providing timely and complete response to government ... investigators' request for documents and access to employees with information."

The code goes on to state that such cooperation does not restrict contractors from conducting an internal investigation, or defending a proceeding or dispute arising under the contract or related to a potential or disclosed violation. Specifically, if a company discovers counterfeit electronic parts, then it should do at least the following as quickly as possible (reference Appendix J, Checklist for Reporting Counterfeits, for detailed information).

- **Document All Steps**: Describe the counterfeit electronic part, how it was purchased and from whom, how it was shipped, how it was determined to be counterfeit, and what subsequent actions were taken. Provide all relevant documents and records.
- **Preserve the Evidence**: Once it is determined that the part is counterfeit (through the receiving inspection or other examination or testing), quarantine the item in secure limited access area, clearly marking it as counterfeit. **Do not return the good**. Maintain a clear chain of custody for the part, documenting when it arrived, how it was used, when and how it was preserved, who had access to it, and any testing or other analysis.

  In addition to the infringing item itself, preserve for later use in a legal proceeding any relevant physical, documentary, or digital evidence acquired in the course of the purchase, acquisition, use, examination, or testing of the counterfeit item. In particular, be sure to retain the original packaging and all documentation received with the part, which may contain valuable details on the item's origin.

  For questions on what to preserve, consult with law enforcement to identify what specific items, records, and documents might have evidentiary value and should be retained. In addition, if there are questions regarding how the parts should be handled or secured, or how long they should be retained, consultation with law enforcement is recommended.
- **Document Contact with the Supplier/Seller**: Provide documentation regarding all representations—both written and verbal—made by the supplier and its employees and representatives, including a copy of the supplier's website as well as emails, texts, and other communications.

  Note that companies or individuals trafficking in counterfeit electronic parts only commit a crime if they know that that they are trafficking in parts with counterfeit trademarks. In other words, it is not enough for someone to sell a counterfeit electronic part; they must also know that the part is counterfeit.

  Thus, once a company determines that it has bought a counterfeit electronic part, it may wish to contact the supplier and ask where the company purchased the electronic part, in which country the part was manufactured, and so on. Preserve any documents or records regarding communications to and from the supplier regarding the counterfeit issue. Even if the supplier

claims that it did not know that the electronic part it sold was counterfeit, those communications could provide evidence of knowledge later if the supplier continues to import or to sell those same counterfeit electronic parts. In addition, the OCM/OEM may be notified of the problem, so it could—if appropriate—send a cease-and-desist letter and/or take legal action against the supplier. The receipt of such a letter or filing of legal action can help remove doubt that the supplier knows that it is trafficking in counterfeit electronic parts.

- **Contact Law Enforcement Right Away**: Early referral to law enforcement is the best way to ensure that evidence of an intellectual property crime is properly secured and that the authorities can fully explore all investigative avenues.

  Law enforcement has many tools to investigate offenses that are unavailable to companies. Moreover, communication with investigative authorities shortly after discovery of a counterfeit electronic part allows an agency or company to coordinate contractual, civil, or administrative proceedings with possible criminal enforcement.

Use of the advisory reporting checklist provided in Appendix J is recommended to organize the information gathered and provide relevant information to the company's law enforcement contact.

6.1.4 Reporting to Customers

Companies should incorporate requirements for customer reporting into their counterfeit control plan in accordance with DFARS 252.246-7007, which specifically identified reporting to the contracting officer. Reporting to customers includes suspect counterfeit parts procured as discrete units and parts supplied to companies that are contained in assemblies. Suspect/counterfeit items that impact customers should be communicated expeditiously and with appropriate due diligence to ensure pertinent facts are provided. Companies operating with a QMS compliant to AS9100 will recognize the requirements for Post Delivery Support[26] and customer communications when problems are detected after delivery. Companies operating to ISO 9001 or other QMS processes may need to enhance customer reporting practices. When reporting suspect/counterfeit incidents to the customer, company processes should include:

- Identification of the suspect/counterfeit item and any impacted customer items.
- Facts regarding the analysis and nature of the evidence associated with the suspect/counterfeit item.
- Investigation results and actions taken.
- Technical analysis of the item application and impact on delivered items.
- Containment information (i.e., pre and post-delivery).
- Corrective actions taken/planned.
- Remediation proposal/plan forward.

6.1.5 Reporting to Industry

Company processes for reporting to industry databases should include all appropriate due diligence including compliance with contractual requirements and consultation with legal counsel. As required by the DFARS, companies must report to GIDEP as part of their process unless other customer or

[26]AS9100C, Quality Management Systems - Requirements for Aviation, Space and Defense Organizations, Paragraph 7.5.1.4

contractual requirements are provided. GIDEP reports should be processed and submitted in accordance with GIDEP requirements which are available at www.gidep.org.

Industry reports should include actionable information such as:

- Information regarding the specific identifiers of the suspect/counterfeit item (e.g., Manufacturer (as marked or labeled on the part), Part Number, Date Code, Lot Code, Serial Numbers).
- Information regarding how the suspect/counterfeit item was discovered.
- Facts regarding the analysis and nature of the evidence associated with the suspect/counterfeit item.
- Investigation results and actions taken.
- Source of supply with all known intermediaries.
- Comments and data from the source of supply.
- Corrective actions taken/planned.

6.1.6 Review of Reporting Databases

Companies should include review of reporting databases in their counterfeit avoidance policy and procedures. Information from reporting databases should be used as part of supplier and component risk assessment process, including pre-procurement and receiving inspection processes, material in stores and delivered items.

Suspect/counterfeit reports require additional assessment beyond the "typical" assessment process. The "typical" process tends to focus on the part and employ an "if used/where used" approach to assess impact and if further action is warranted. While "if used/where used" remains important in suspect/counterfeit report assessment it is only half of the needed due diligence.

Suspect/counterfeit reports should also be assessed for potential risk or impacts that may be associated with the organizations use of the supplier(s) identified in the report. The supplier's response to a reported incident as well as any trends that may be present are important factors to consider in making a determination if further action is warranted.

6.2 Quarantining

6.2.1 Requirements

The FY2012 NDAA and the DFARS requires contractors that supply electronic parts or systems that contain electronic parts to establish policies and procedures to eliminate counterfeit electronic parts from the defense supply chain. The requirement states in part that contractor "policies and procedures shall address the reporting and quarantining of counterfeit electronic parts and suspect electronic parts".[27] The DFARS state specifically, "Counterfeit electronic parts and suspect counterfeit

[27] H.R.1540 National Defense Authorization Act for FY2012, Section 818, Detection and Avoidance of Counterfeit Electronic Parts (e), (2), (vi)

electronic parts shall not be returned to the seller or otherwise returned to the supply chain until such time that the parts are determined to be authentic."[28]

Company policy and procedures should address the quarantine and control of suspect/counterfeit items. The entire lot of suspect/counterfeit items should be quarantined in a secure limited access area. The parts and or part packaging should be marked appropriately to clearly identify the items as suspect/counterfeit. When items are removed from the quarantine, a chain of custody process should be used to ensure material control and accountability.

A complete documentation package should be compiled and available for suspect/counterfeit items in quarantine. The documentation should include all original documents associated with the part including:

- Manufacturer information
- Part procurement/acquisition traceability
- Copy of the purchase order
- Any and all correspondence between the buyer and supplier
- Part documentation from the supplier
  - Certificate of Compliance
  - Certificate of Conformance
  - Inspection and test results/reports
- Any additional inspection and test results
- Any correspondence with the original manufacturer

6.2.2 Disposition

Material Returns: Any return of suspect/counterfeit parts provides a risk that the parts could re-enter the supply chain. It is important that contractors DO NOT return the counterfeit items to the supplier as prohibited by the DFARS. They may be used as evidence if the government decides to take legal action, your legal counsel may issue a legal hold to preserve such evidence, and quarantine ensures that the parts will not be put back into circulation.

Scrap Process: Suspect/counterfeit parts should be approved for disposal prior to destruction; consult your legal counsel. The approval process should ensure all legal and administrative obligations have been met. If approved, the scrap process used for suspect counterfeit and counterfeit parts should ensure the parts are disposed of in a manner that ensures the parts cannot be reused or refurbished in any way. The preferred scrap process is complete destruction of the part such that there is no possibility for re-entry into the supply chain other than for raw material reclamation.

[28] See http://www.acq.osd.mil/dpap/dars/dfars/html/current/252246.htm#252.246-7007, sub-section (c)(6).

7. Flow Down of Counterfeit Avoidance and Detection Requirements

DFARS rule, 48 CFR 252.246-7007(c)(9) requires the "Flow down of counterfeit detection and avoidance requirements, including applicable system criteria provided herein, to subcontractors at all levels in the supply chain that are responsible for buying or selling electronic parts or assemblies containing electronic parts, or for performing authentication testing."

Requirements flow down to suppliers should account for risks of potential counterfeit part quality escapes where the subcontractor's or service provider's offering will consist of on-hand materiel inventory in addition to new materiel procurements. Depending on the extent of due diligence applied to on-hand materiel, requirements flow down should include additional due diligence. While the DFARS requires flow down of the substance of the clause to "in subcontracts, including subcontracts for commercial items, for electronic parts or assemblies containing electronic parts," the following sections offer further best practice guidance.

7.1 Scope of Requirements

The focus of this section is the flow down of requirements within the supply chain as referenced in Figure 1-1. Requirements flowed down to suppliers should focus on the predominant means by which counterfeit electronic parts find their way into the supply chain:

- Procurement at any point in the supply chain from other than an authorized supplier
- Procurement from unauthorized suppliers without sufficient supplier selection and counterfeit avoidance/detection practices

Requirements flowed down to suppliers should embody the central tenets to counterfeit prevention:

- Apply supplier preferences for electronic parts purchased from authorized supplier,
- Perform due diligence to avoid counterfeits when purchases from sources of supply other than authorized suppliers are necessary, and
- In the event that suspect counterfeit or counterfeit electronic parts are discovered, (a) disposition that precludes their use or reentry into the supply chain, and (b) notify supplier's customer(s), government and industry of the finding.

7.2 Types of Suppliers Versus Appropriate Requirements Flow Down

Counterfeit avoidance and detection requirements should be flowed down to the following types of suppliers:

- Prime contractors and integrators of systems containing electronic parts.
- OEMs that supply equipment or assemblies containing electronic parts.
- Subcontractors that repair or maintain equipment or assemblies containing electronic parts, or supply electronic parts.
- Contract Manufacturers (CM) and Electronic Manufacturing Service (EMS) providers that supply equipment or assemblies containing electronic parts.
- Third Party Logistics (3PL) providers of services associated electronic parts.
- Distributors of electronic parts.

Counterfeit avoidance and detection requirements flowed down to suppliers should be context sensitive and relevant for the type of supplier. For example, requirements directed to a prime contractor or upper tier subcontractor should differ from requirements directed to an electronic part distributor. In the case of a prime contractor or upper tier subcontractor the flow down should include all three of the central tenets to counterfeit prevention (see Section 7.1). However, in the case of electronic part distributor, appropriate requirements could be for the distributor to (1) supply only product for which it is an authorized supplier or to supply products acquired from a supplier that is an authorized supplier, (2) provide traceability documentation, (3) do not supply products returned by other customers, and (4) report if suspect counterfeit or counterfeit parts are encountered.

Counterfeit avoidance and detection requirements flowed down to suppliers should include an expectation that these requirements are in turn be flowed to its suppliers. There should be sufficient flow down of requirements to provide counterfeit risk protection. When flow down throughout the supply chain is not achieved, the end customer should be notified.

7.3 Counterfeit Prevention Clauses and False Claims Act Considerations

According to noted experts in procurement fraud and criminal prosecutions associated with counterfeiting, selling counterfeit electronic parts to the military or other government agencies can result in civil (Federal False Claims Act) and administrative (Suspension and Debarment) action as well as criminal prosecution. A criminal prosecution will focus on the devices sold (including all part markings) and all representations (verbal and in writing) made to the buyer by the seller and its employees and representatives. Such charges could include Trafficking in Counterfeit Goods or Services, (18 U.S.C. 2320), Mail Fraud (18 U.S.C. 1341), Wire Fraud (18 U.S.C. 1343), and Conspiracy (18 U.S.C. 371).

If a supplier accepts orders subject to counterfeit parts prevention clauses from its customer in support of a U.S. government DOD contract[29], but does not implement systems to comply with the requirements of the clause, the supplier can be held liable under the civil False Claims Act (FCA) for submitting invoices for payment even if no counterfeit parts are delivered to the prime contractor.

Damages do not need to be proven to violate the civil FCA. Therefore, the prime contractor's or subcontractor's mere submission of an invoice for payment, with the knowledge it does not have systems in place to comply with the broad counterfeit parts prevention clause, is arguably a false claim.

7.4 Electronic Part Obsolescence Considerations

Defense and aerospace products are particularly vulnerable to counterfeit electronic parts due to part 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. Recognizing this risk, DFARS 252.246-7007(c)(12) requires "Control of obsolete electronic parts in order to maximize the availability and use of authentic, originally designed, and qualified electronic parts throughout the product's life cycle."

In order to reduce the likelihood of having to purchase parts through riskier supply chains, defense and aerospace electronics producers and their customers should recognize the need to proactively manage the life cycle of electronic products versus the life cycles of the parts used within them. When

[29]Note well that NASA may implement similar legislation as proposed in H.R. 4412, dated April 7, 2014.

assessing product offerings and proposals for production and support contracts, companies should seek information concerning the potential demand for obsolete parts associated with the product offering. Assess plans to either assure authorized sources of supply for obsolete electronic parts, or plans to implement design modifications to eliminate obsolete electronic parts. Counterfeit avoidance and detection requirements flowed down to suppliers should be based on the outcome of this assessment and specific plans to modify equipment in order to eliminate obsolete parts, or to proceed with a mutually agreed upon risk mitigation plan for acquiring obsolete parts from independent distributors and other sources that are not authorized by the OCM (e.g., Government Furnished Material (GFM)/Customer Furnished Material (CFM), DLA, customer support contractors that acquire parts on their behalf).

7.5 Counterfeit Prevention and On-Hand Material Inventory

Subcontractors and service providers (e.g., contract manufacturers, EMS) may have accumulated inventory to support long term requirements before the counterfeit parts threat and associated supply chain issues were well understood. Some acquired inventory through mergers and acquisitions without intimate knowledge of the history of that inventory. Though poised to apply counterfeit prevention due diligence for materiel procurements going forward, some may not have performed the same or similar due diligence for its entire inventory. Issues to consider when devising requirements to flow down to suppliers should include the following:

- Relevant procurement history from authorized suppliers may be missing for parts in inventory or parts do not have traceability to the OCM.
- Parts acquired from unauthorized suppliers may not be segregated from parts acquired from authorized suppliers.
- Electronic assemblies in inventory may contain parts where procurement history is unknown or untraceable to the OCM.

In response to a comment concerning parts already in a contractor's inventory, provided with the release of DFARS 246.870[30], it indicates that these parts are subject to the same requirements, such as traceability and documentation, as are new procurements. These requirements apply if the parts were not procured in connection with a previous DOD contract.

7.6 Notification of Purchases from Unauthorized Suppliers

Prime and sub-tier contractors should flow down a requirement for suppliers to notify them when the supplier plans to purchase or otherwise use electronic parts acquired from other than an authorized supplier. Prime and sub-tier contractors should also consider flowing down a requirement for the supplier to seek approval for such purchases, to disclose the rationale for such purchases, and to disclose the specific plan to avoid the purchase of counterfeit electronic parts.

7.7 Shipments from Authorized Suppliers Consisting of Product Returns

Reported cases of counterfeit parts supplied by authorized suppliers are very rare. Though authorized suppliers supply products acquired directly from the OCM, they occasionally accept product returns from their customers. Cases have been reported where a customer did not return the same authentic products acquired from an authorized supplier, but, instead, returned other products that were counterfeit. If an authorized supplier does not apply sufficient due diligence for product returns from

[30]Federal Register Vol. 79, No. 87 at p. 26099

customers, counterfeit parts can be inadvertently introduced into its inventory. Product returns generally comprise a very small subset of an authorized supplier's total shipments on an ongoing basis. While it is reasonable to assume the risk of counterfeit parts escapes through authorized distribution is very low, a review of the authorized supplier's product return acceptance practices (e.g., verification of returns, identification, and segregation, if returned to inventory) is a prudent precaution. Prime and sub-tier contractors should consider forbidding authorized suppliers from shipping products consisting of products returned by other customers, including aftermarket manufacturers.

8. Training of Personnel

DFARS rule, 48 CFR 252.246-7007(c)(1) requires “The training of personnel” as an integral part of a contractor’s counterfeit electronic part detection and avoidance system.

8.1 General Awareness

Counterfeit parts training serves a variety of purposes depending on the maturity and familiarity of the organization’s counterfeit parts mitigation process. A training program should incorporate at a minimum general awareness training where participants come away with a basic understanding of the electronic parts counterfeit problem. This level of training may be appropriate for personnel that are not directly involved in roles associated with the counterfeit prevention strategy.

8.1.1 Training for Specific Areas

A more advanced training program should be created by going in depth into select areas of the counterfeit problem and tailoring to specific groups with counterfeit prevention responsibilities. For example, training can be generated specifically for procurement, quality inspectors, and engineering personnel. For procurement personnel topics and concepts such as an approved supplier or vendor list and policies and procedures relative to procuring from such lists should be included in the material. For quality inspectors, reviewing actual supplier documentation, examples of manufacturer logos and a hands-on inspection of actual components and reporting requirements in the event suspect components are found would provide the most benefit and impact. Any counterfeit training geared towards engineering personnel should include discussions on the risk of encountering counterfeit parts with heritage designs and obsolete components. As a final example of area specific training, legal departments should be trained to understand the implications of obsolescence, the elements of the new law, the reporting requirements (including mandatory reporting to the government where required), and how to ensure terms and conditions are negotiated for compliance with flow down requirements.

Lastly, training can also be in the form of a short overview presentation for upper management.

The material can be designed in modules (i.e., a basic awareness module, an inspection training module) to allow mixing and matching to better meet schedule and budget constraints. Organizing the training in modules also helps facilitate the creation of more specialized briefings and training if the need arises.

8.1.2 Training Requirement

Training should be integrated in the basic employee development plan and be managed accordingly and include aspects such as refresher/recertification requirements. This subject matter is a beneficial addition to the typical new hire/orientation training. It is suggested that retraining be implemented every two years.

8.1.3 Terms and Definitions

Basic terms and concepts that will be used in the main body of the training document should be covered early in the training material. This section can be in a simple list format such as found in AS5553. The material can also be presented in an interactive flowchart where the instructor steps through and defines each element in the chosen process. An example of this would be to flow the

procurement process and define elements such as OCM, authorized supplier, franchised distributor, OEM, unauthorized supplier, approved supplier, and independent distributors.

8.1.4 Mechanics of Counterfeiting

This section of the training usually proves to be an eye opener for individuals who have not had much exposure or training to the electronics parts counterfeit problem. Topics such as part obsolescence, the role of E-Waste as a contributor to the problem, potential sources and methods to counterfeit parts should be included in this area of the training. Case studies, news clippings, and documentary videos also serve as powerful and effective tools that enhance this part of the training.

8.1.5 Risk Mitigation

A key aspect and probably the most important subject that should be addressed in any counterfeit training is a discussion of the risks involved and the possible steps to mitigate risk. The criticality of obsolescence management, supplier selection and management, and the consequences of a poor procurement process should be the prime focus in this part of the course material.

The subject can also be made more relevant with a discussion on how the different departments and personnel are integrated across multiple organizations. For example, design engineering, procurement, incoming inspection, and counterfeit parts management may contribute to minimizing (or exacerbating) the risk of introducing counterfeit parts into the end product.

8.1.6 Counterfeit Mitigation Processes

The processes described in the following paragraphs play a key role in mitigating counterfeit risk and lend themselves to a thorough examination in this section of counterfeit parts training. Furthermore, it is beneficial to engage the training participants in evaluating their own organization's performance in managing the processes described below.

1. Procurement process – a discussion of the type of policies and procedures helpful in mitigating risk and what is actually in place in one's own organization usually brings to light strengths and weaknesses. The following related questions also serve as enlightening and educational:
    a. Is the organization free to procure from any source?
    b. What restrictions and oversight are present?
    c. Does the organization have an approved supplier list and what considerations are there relative to counterfeit parts mitigation in creating the pool of approved suppliers?
    d. How are the organization's suppliers assessed and audited?
2. Authentication/validation process – a discussion of the inspections and tests specific to the detection of counterfeit parts and systems and what is actually in place in one's organization is also an important subject. For example:
    a. What inspection criteria is in place?
    b. Does the organization inspect all or some of the goods?
    c. Are there any special inspection tools or equipment used?
    d. How is traceability and provenance verified?

3. Reporting and Incident Response process – a discussion of the steps an organization may be required to take in the event counterfeit product is discovered in the course of doing business. Considerations include:
    a. What are the avenues for reporting a counterfeit occurrence?
    b. What contract clauses come into play in the event suspect counterfeit goods are acquired from a supplier?
    c. What processes are in place in one's organization if suspect products are found to have passed inspection and are in stores or installed in an assembly.
    d. What steps are to be taken if a suspect counterfeit part is discovered in product that has been delivered to a customer?

8.1.7 Requirements

A review of the various industry standards written for counterfeit parts mitigation and a review of the various laws and regulations, policies and procedures that may be applicable to the participant's organization as well as internal counterfeit mitigation policies and procedures are key elements of a counterfeit training program. The FY2012 NDAA, SAE Standard AS5553, TOR-2006(8583)-5235, and TOR-2006(8583)-5236 are notable examples of the above. Anchoring the counterfeit mitigation and training process to actual requirements shows the issue from a different perspective that may be beneficial to the participants and may help identify compliance gaps that could be potential audit findings.

8.1.8 Miscellaneous

Incorporating a hands-on inspection of actual components during the training program, if possible, engages the participants and can be used as an educational tool to emphasize some of the visual anomalies found on suspect counterfeit parts. There are also numerous videos and actual case studies that should be incorporated into the training to help illustrate the concepts covered in the material.

Examples of training material, best practices and lessons learned, and other useful information can be found in Appendix A, *Training Links*; Appendix B, *Best Practices and Lessons Learned*; Appendix C, *Observations and Driving Philosophies*; and Appendix D, *Case Studies*.

9. Maintaining Currency for Counterfeiting Information and Trends

DFARS rule, 48 CFR 252.246-7007(c)(10) states that a contractor's counterfeit electronic part detection and avoidance system shall include a "process for keeping continually informed of current counterfeiting information and trends, including detection and avoidance techniques contained in appropriate industry standards, and using such information and techniques for continuously upgrading internal processes."

Continuous assessment and improvement of the counterfeit prevention system is necessary to stay ahead of the threat and to keep processes at their best. The methodologies employed by unethical companies to counterfeit electronic parts continue to evolve and become more sophisticated. Companies need to maintain awareness of the techniques being used by counterfeiters and methods to combat these techniques. As stressed throughout this document the preferred and primary method to preclude the counterfeit electronics part problem is to procure only from the OCM or current design authority, including an authorized aftermarket manufacturer or suppliers that obtain parts exclusively from one or more of these sources. However, when this is not possible, periodic analysis of the threat, assessment of company processes, and the continual improvement of company prevention techniques are necessary.

Showing continuous improvement and keeping informed of current counterfeiting information and trends can be accomplished in many ways. The following is a list of possible methods to meet the DFARS requirement. Objective evidence for the list below will be helpful to show that the contractor is maintaining currency and continually strengthening internal processes.

- Perform a "gap analysis" and revision of the company command media as a result of new or revised laws, government specifications, or industry standards.
- Evaluate and freshen company training programs annually based on the evolving threat or requirements changes.
- Conduct internal audits to ensure employees are performing to all counterfeit prevention system requirements.
- Develop a set of measures and metrics to ensure success key parameters are monitored and trended for potential preventative action.
- Conduct periodic analysis of GIDEP documents (www.gidep.org) and other industry sources associated with counterfeit electronic parts.
- Implement a closed-loop system that updates and strengthens command media based on counterfeit escapes, near-misses, audit findings, metric violations, and lessons learned.
- Join industry organizations that are on the cutting edge of developing prevention techniques or that are chartered with revising an industry standard.
- Attend seminars and workshops. Examples include:
    - University of Connecticut Center for Hardware Assurance, Security, and Engineering (CHASE) – https://www.chase.uconn.edu/
    - University of Maryland Center for Advanced Life Cycle Engineering (CALCE) – http://www.calce.umd.edu/
    - Hardened Electronics And Radiation Technology (HEART) Conference – http://www.heart-conference.org/

- The Aerospace Corporation Space Parts Working Group – http://www.cvent.com/events/2014-space-parts-working-group/event-summary-50472b2a31c6490ea33ae2f9c884e5b2.aspx (2014 Working Group link provided)

- Reference the Department of Justice (DOJ) National Intellectual Property Rights (IPR) Coordination Center for the latest on prosecutions of counterfeiters – www.iprcenter.gov
- Periodically perform a risk assessment on company processes and present the results and improvement recommendations to leadership.

10. Acronyms

3PL	Third Party Logistics
ABPMPL	As-Built Parts, Materials and Processes List
AC	Alternating Current
AFOSI	Air Force Office of Special Investigation
AIA	Aerospace Industries Association
ANSI	American National Standards Institute
ASL	Approved Supplier List
CAR	Corrective Action Request
CBP	Customs and Border Protection
CCPIS	Computer Crime & Intellectual Property Section
CDRLs	Contract Data Requirements List
CFM	Customer Furnished Material
CFR	Code of Federal Regulations
CID	Criminal Investigation Command
CM	Contract Manufacturer
CoC	Certificate of Conformance
CoC/T	CoC Supply Chain Traceability
COTS	Commercial-Off-The-Shelf
DC	Direct Current
DCIS	Defense Criminal Investigative Service
DCMA	Defense Contract Management Agency
DFARS	Defense Federal Acquisition Regulation Supplement
DID	Data Item Description
DLA	Defense Logistics Agency
DMEA	Defense Microelectronics Agency
DoD	Department of Defense
DoDI	Department of Defense Instruction
DOE	Department of Energy
DPA	Destructive Physical Analysis
ECIA	Electronic Component Industry Association
EDX	Energy Dispersive X-Ray (verify)
EEEE	Electric, Electronic, and Electro-mechanical, Electro-optical
ELDRS	Enhanced Low Dose Rate Sensitivity
EMS	Electronic Manufacturing Service
EPLS	Excluded Parties List System
ESD	Electro-Static Discharge
FAA	Federal Aviation Administration
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FCA	False Claims Act
FET	Field Effect Transistor
FY	Fiscal Year
GFM	Government Furnished Material
GFSC	Goddard Space Flight Center
GIDEP	Government-Industry Data Exchange Program
GPO	Government Printing Office
HIS	Homeland Security Investigations
IC	Integrated Circuit

IPR	Intellectual Property Rights
ISO	International Standards Organization
IUID	Item Unique Identification
JDRS	Joint Deficiency Reporting System
JEDEC	Joint Electronics Device Engineering Council
JIT	Just-In-Time
LDC	Lot Date Code
MAIW	Mission Assurance Improvement Workshop
MDA	Missile Defense Agency
MSL	Moisture Sensitivity Level
MTE	Measuring & Test Equipment
NASA	National Aeronautics and Space Administration
NCIS	Naval Criminal Investigative Service
NCSL	National Conference of Standards Laboratories
NDAA	National Defense Authorization Act
NIST	National Institute of Standards & Technology
NRO	National Reconnaissance Office
NSS	National Security Space
OCM	Original Component Manufacturer
OEM	Original Equipment Manufacturer
OQE	Objective Quality Evidence
OSHA	Occupational Safety & Health Administration
PDREP	Product Deficiency Reporting and Evaluation Program
PM&P	Parts, Materials & Processes
PMPCB	Parts, Materials & Processes Control Board
PPE	Personal Protective Equipment
PUMPS	Parts, Units, Materials, Processes and Systems
QA	Quality Assurance
QMS	Quality Management System
QSLD	Qualified Suppliers Listing of Distributors
QTSL	Qualified Testing Suppliers Listing
RTL	Responsible Test Laboratory
SAE	Society of Automotive Engineers
SAM	System for Award Management
SCD	Specification Control Drawing
SEM	Scanning Electron Microscope
SI	Systems of Units
SMC	Space and Missiles Systems Center
SME	Subject Matter Expert
SOW	Statement of Work
SPC	Statistical Process Control
SQIC	Space Quality Improvement Council
SSC	Space Suppliers Council
TOR	Technical Operating Report
URL	Universal Resource-Locators
USAF	United States Air Force
USD/AT&L	Under Secretary of Defense for Acquisition, Technology & Logistics
USD/I	Under Secretary of Defense for Intelligence
XRF	X-Ray Fluorescence

11. References

H.R. 1540, FY2012 NDAA, §818(e)	Improvement of Contractor Systems for Detection and Avoidance of Counterfeit Electronic Parts
H.R. 4310, FY2013 NDAA, §833	Contractor Responsibilities in Regulations Relating to Detection and Avoidance of Counterfeit Electronic Parts

FAR Case 2013-002	Expanding Reporting of Nonconforming Supplies
FAR 52.203-13	Contractor Code of Business Ethics and Conduct
FAR 2.101	Definitions
FAR 3.10	Contractor Code of Business Ethics and Conduct

DFARS Rule, 48 CFR 246.870	Contractors' Counterfeit Electronic Part Detection and Avoidance Systems
DFARS Rule, 48 CFR 252.246-7007	Contractor Counterfeit Electronic Part Detection and Avoidance System
DFARS 252.211-7003	Item Unique Identification and Valuation

DoDI 4140.67	DoD Counterfeit Prevention Policy
DoDI 5200.39	Critical Program Information (CPI) Protection within the Department of Defense

MIL-STD-202	Test Method Standard, Electronic and Electrical Component Parts
MIL-STD-750	Test Method Standard for Semiconductor Devices
MIL-STD-883	Test Methods and Procedures for Microcircuits
MIL-STD-3018	Parts Management
MIL-STD-1546	Parts, Materials, and Processes Standardization, Control, and Management Program for Space and Launch Vehicles
MIL-STD-1580	Department of Defense Test Method Standard Destructive Physical Analysis for Electrical, Electronic, and Electromagnetic Parts
MIL-PRF-38535	Integrated Circuits (Microcircuits) Manufacturing, General Specification for

Aerospace TOR-2006(8583)-5235	Parts, Materials, and Processes Control Program for Space Vehicles
Aerospace TOR-2006(8583)-5236	Technical Requirements for Electronic Parts, Materials, and Processes Used in Space Vehicles

NASA MFSC-STD-3619	MSFC Counterfeit Electrical, Electronic, and Electromechanical Parts Avoidance, Detection, Mitigation, and Disposition Requirements for Space Flight and Critical Ground Support Hardware

ISO-9001	Quality Management System - Requirements
ISO/IEC 17025	General Requirements for the Competence of Testing and Calibration Laboratories

AS5553	Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition

AS6081	Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition Distributors
AS6171 (*proposed*)	Test Methods Standard; Counterfeit Electronic Parts
AS6174	Counterfeit Material; Assuring Acquisition of Authentic and Conforming Material
ARP6178	Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors
AIR6273 (*proposed)*	Terms and Definitions – Fraudulent/Counterfeit Electronic Parts
AS6301 (*proposed)*	Compliance Verification Criterion Standard for SAE AS6081, Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition – Distributors
AS6462	AS5553 Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria
AS6496 (*proposed*)	Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition – Authorized/Franchised Distribution
AS9003	Inspection and Test Quality System
AS9100	Quality Management Systems – Requirements for Aviation, Space and Defense Organizations
AS9120	Quality Management Systems – Aerospace Requirements for Stockist Distributors
SAE TB-003	Counterfeit Parts & Materials Risk Mitigation
ANSI/ESD S20.20	For the Development of an Electrostatic Discharge Control Program for Protection of Electrical and Electronic Parts, Assemblies and Equipment (Excluding Electrically Initiated Explosive Devices)
ANSI/NCSL Z540.3-2006	Requirements for the Calibration of Measuring and Test Equipment
ANSI/EIA-933-A	Standard for Preparing a COTS Assembly Management Plan
ANSI/EIA-4899-2002	Standard for Preparing an Electronic Components Management Plan
TechAmerica STD-0016	Standard for Preparing a Diminishing Manufacturing Sources and Material Shortages (DMSMS) Management Plan

FAA AC 00-56	Voluntary Industry Distributor Accreditation Program

JEDEC JESD 31	General Requirements for Distributors of Commercial and Military Semiconductor Devices
JEDEC J-STD-033	Handling, Packing, Shipping and Use of Moisture/Reflow Sensitive Surface Mount Devices
JEDEC JESD 625	Requirements for Handling Electrostatic-Discharge-Sensitive (ESDS) Devices

Telcordia GR-468-CORE	Generic Reliability Assurance Requirements for Optoelectronic Devices Used in Telecommunications Equipment

CCAP-101	Counterfeit Components Avoidance Program, Certification For

SEMI T20-0710	Specification for Authentication of Semiconductors and Related Products
SEMI T20.1-1109	Specification for Object Labeling to Authenticate Semiconductors and Related Products in An Open Market

SEMI T20.2-1109	Guide for Qualifications of Authentication Service Bodies for Detecting and Preventing Counterfeiting of Semiconductors and Related Products

EIA/ECA-CB21	Counterfeit Passive Components
IEC/TS 62668-1	Process Management for Avionics – Counterfeit Prevention – Part 1: Avoiding the Use of Counterfeit, Fraudulent and Recycled Electronic Components
IEC/TS 62668-2 (*proposed*)	Process Management for Avionics – Counterfeit Prevention – Part 2: Managing Electronic Components from Non-Franchised Sources

Appendix A. Training Resources

This appendix includes links to publically accessible NASA and MDA training packages that may be downloaded and tailored when improving or establishing a counterfeit prevention program.

NASA Counterfeit Awareness Training – Basic

http://mttc.jpl.nasa.gov/files/COUNTERFEIT%20PARTS%20AWARENESS%20TRAINING_Basic.pptx

NASA Counterfeit Awareness Training - Intermediate

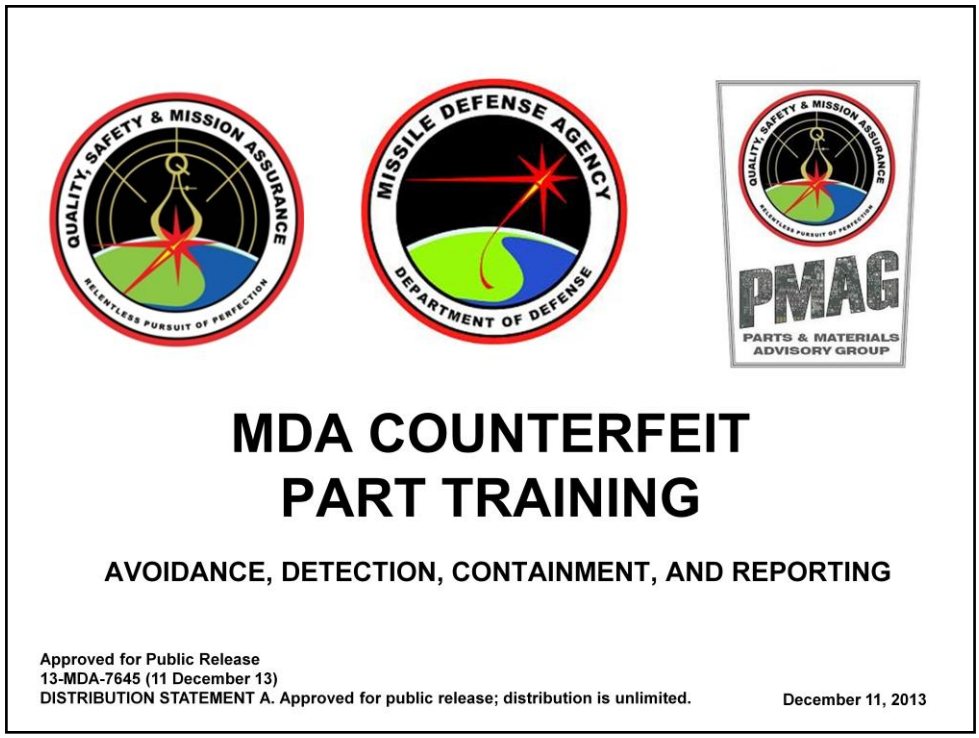
http://mttc.jpl.nasa.gov/files/COUNTERFEIT%20PARTS%20AWARENESS%20TRAINING_Intermediate.pptx

NASA Counterfeit Awareness Training – Inspection

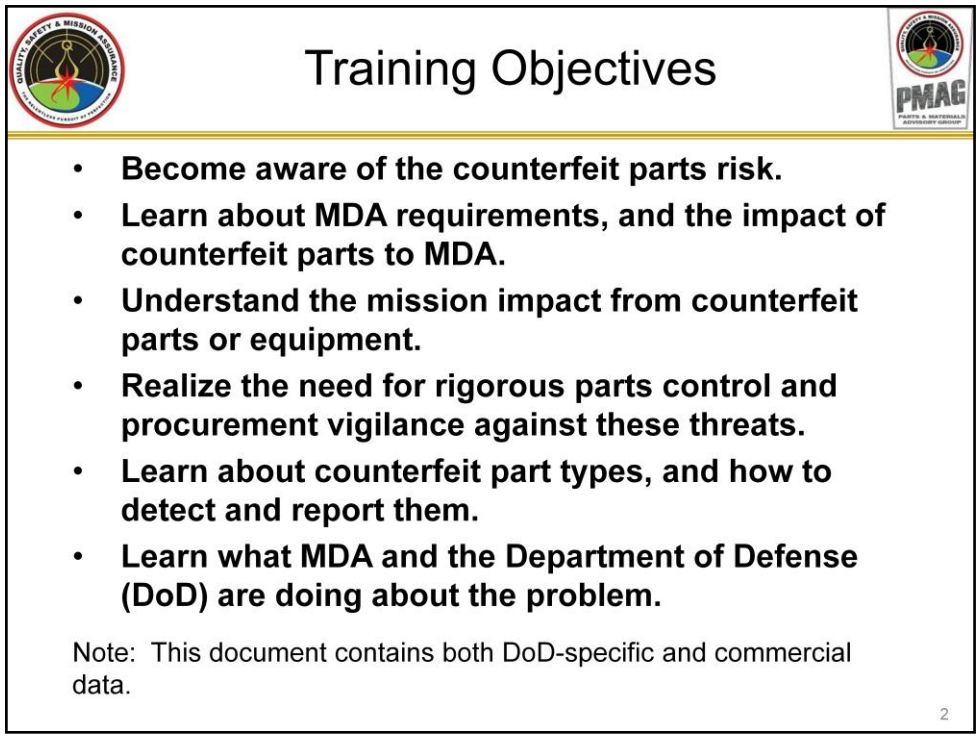
http://mttc.jpl.nasa.gov/files/COUNTERFEIT%20PARTS%20AWARENESS%20TRAINING_Inspection.pptx

MDA Counterfeit Part Training – Avoidance, Detection, Containment, and Reporting

MDA_Counterfeit_Training_(December_11_2013)_-_MAIW_Release

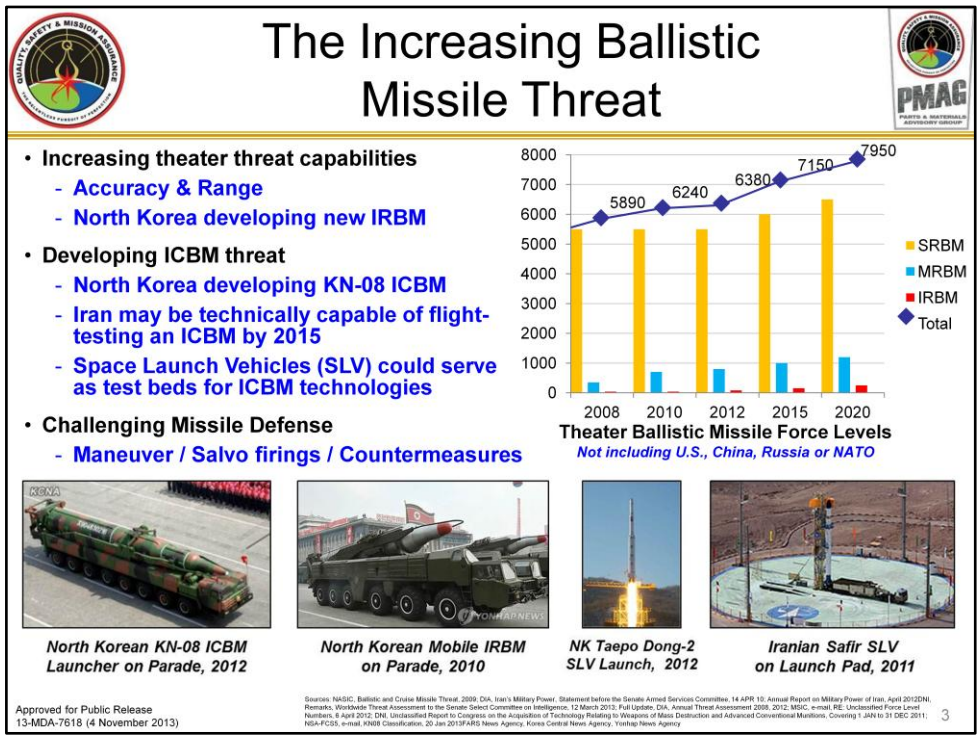


This presentation contains information pertaining to the avoidance, detection, containment, and reporting of counterfeit parts. It represents experience gained through many hours of work by employees of the Missile Defense Agency, and is intended to aid all affected MDA and MDA Contractor personnel, including - but not limited to - purchasers, program managers, engineers, inspectors, and quality personnel.



After completing this training program, you should be aware of the very real risk that counterfeit parts manifest to the United States military, including knowledge of the Missile Defense Agency's experience with counterfeit parts. You should have a better understanding of how counterfeit parts can dramatically impact MDA's various programs. You should understand why it is so important to be diligent in how we buy parts, especially who we buy them from. You will learn about the many types of counterfeit parts, and which inspections and tests can be most counted on to detect these parts. Lastly, you will learn about the current anti-counterfeit requirements and efforts in place by MDA and the Department of Defense, or DoD.

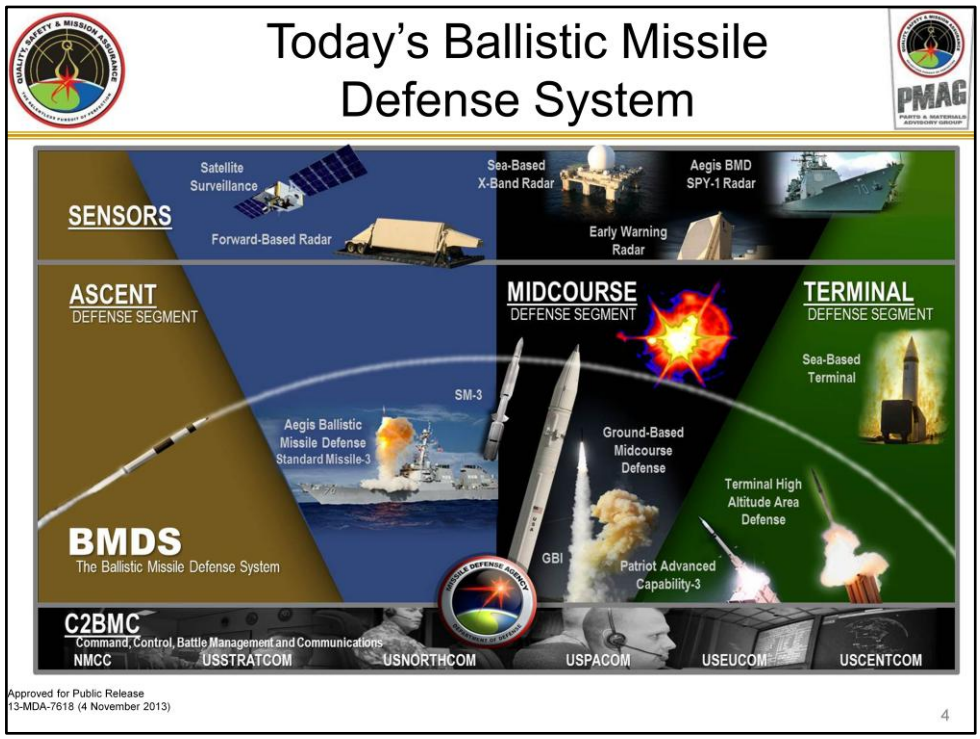
Some of the information you will see in this presentation involves data gathered from the commercial sector, but most of it involves parts and materials that can be or are used in DoD hardware.



First, a little information about the Missile Defense Agency. Founded in 1983 as the Strategic Defense Initiative, there are several reasons why MDA remains a vital part of our defense capabilities.

The number of ballistic missiles of all ranges continues to increase every year, as the chart on the right indicates. If we exclude Russia, China, and the NATO member countries, the majority are short and medium range missiles. However, as potential adversaries like North Korea and Iran continue development of longer range missiles, the threat to the United States and our allies continues to grow.

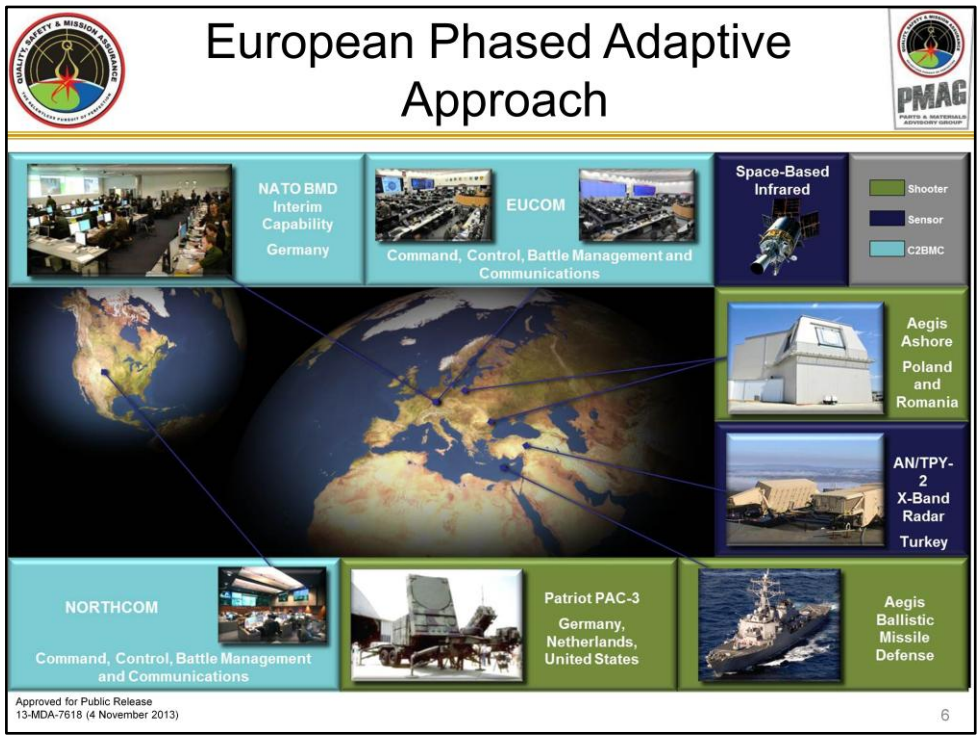
The photos on the bottom show examples of missiles either currently in development or recently deployed.



Missile defense technology being developed, tested and deployed by the United States is designed to counter ballistic missiles of all ranges—short, medium, intermediate and long. Since ballistic missiles have different ranges, speeds, size and performance characteristics, the Ballistic Missile Defense System is an integrated, "layered" architecture that provides multiple opportunities to destroy missiles and their warheads before they can reach their targets. The system's architecture includes ground-, sea-, and space-based networked sensors, ground- and sea-based radars for target detection and tracking, ground- and sea-based interceptor missiles for destroying incoming threats, and a command, control, battle management, and communications network providing the operational commanders with the needed links between the sensors and interceptor missiles.

Missile defense elements are operated by United States military personnel from U.S. Strategic Command, U.S. Northern Command, U.S. Pacific Command, U.S. Forces Japan, U.S. European Command and others.

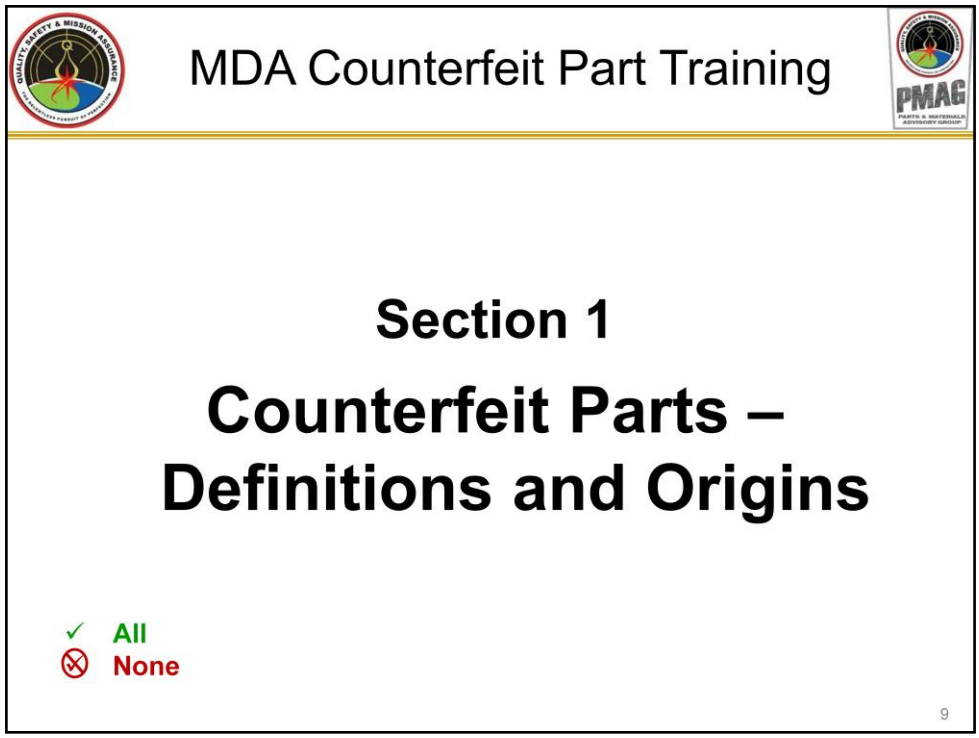
This graphic shows the integrated network charged with protecting the United States from the ballistic missile threat. U.S. Northern Command and Pacific Command personnel man the C2BMC system, utilizing data from strategically-located sensors to identify all incoming threats. The C2BMC determines a plan of action, and reacts accordingly by launching interceptors with the greatest chance of destroying the threats. The ground-based midcourse defense system is the primary defense asset for protecting the United States.



MDA assets are also deployed to help defend our European allies. Along with U.S. Northern Command, NATO and European allies help assess and react to the ballistic missile threat. Sea-based Aegis, land-based Aegis Ashore, and the Patriot PAC-3 missile batteries are the primary defense assets for this arena. MDA is working with partner countries like Poland, Romania, Turkey, Germany, and the Netherlands to establish a robust missile defense system.

In the Asia-Pacific region, U.S. Pacific Command and Northern Command monitor the threat. Radars located in Japan and aboard Aegis-equipped ships identify incoming missiles. Strategically-placed Aegis, Patriot, and THAAD interceptors will stand ready to act to protect this region.

MDA headquarters is located in Fort Belvoir, VA, with the main workforce located in Huntsville, AL. There are several additional major installations within the continental U.S. and Hawaii, that concentrate on command and control, sensors, and launch facilities. MDA also uses hundreds of U.S. contractors to design and build this complex, integrated defense system.

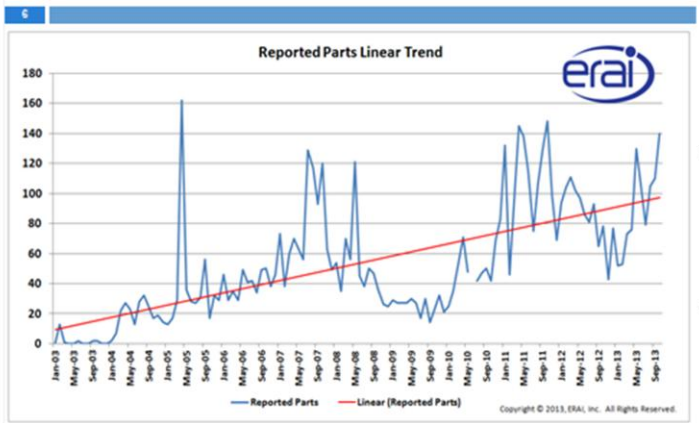


In this section, you should learn the basic facts about counterfeit parts and materials. It will concentrate heavily on counterfeit electronic parts. Counterfeit mechanical parts and materials are also a serious risk to the MDA ballistic missile defense system, and will be discussed. However, it is generally recognized that electronic parts are more widely counterfeited, and also have the greatest potential for malicious tampering. Therefore, electronic parts will be the main focus of this training course.

At each section title, there will be a listing on the bottom that indicates the personnel job types recommended to review that section.

Counterfeiting, An Upward Trend

Reported Parts Linear Trend

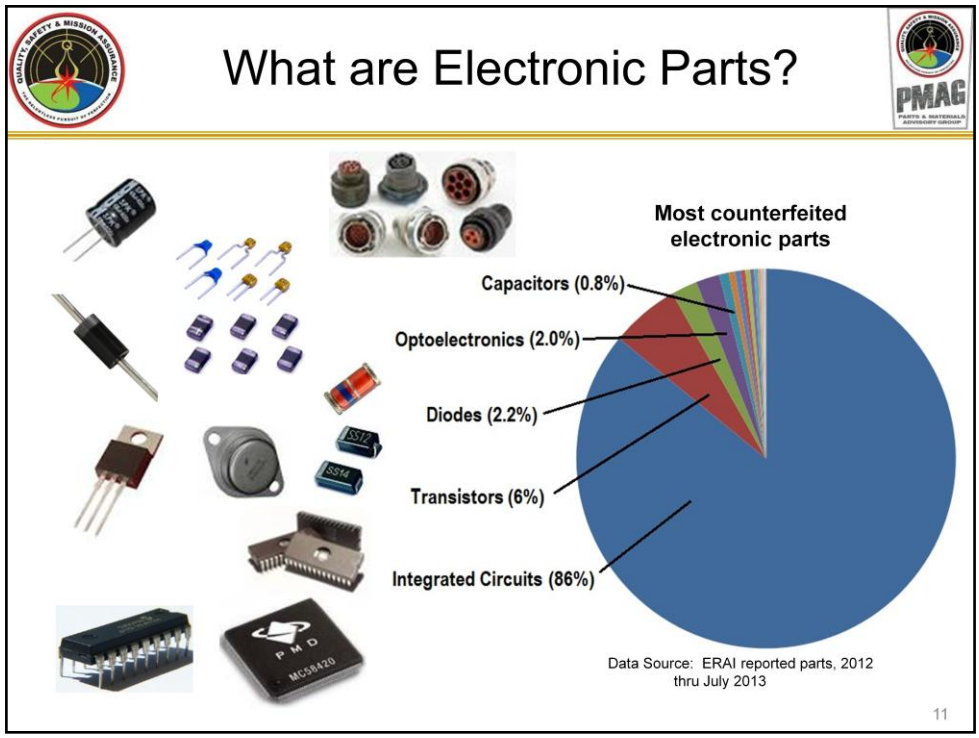


Preliminary data, courtesy ERAI.

ERAI notes a marked increase in counterfeit part reporting in the past 10 years.

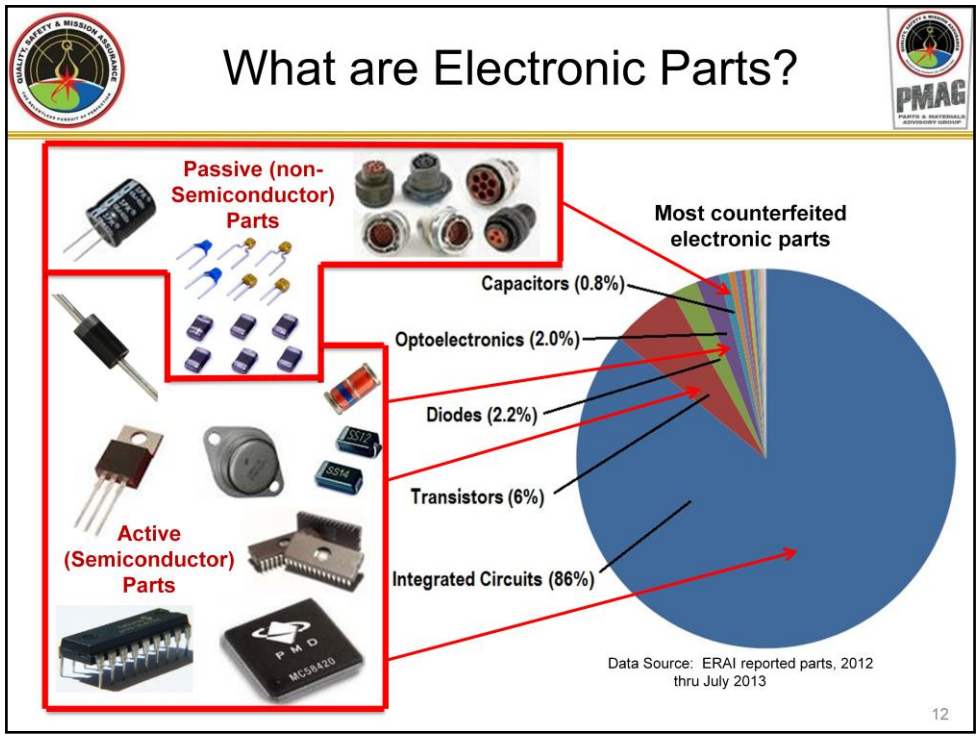
10

Most people agree that counterfeiting has been on the rise for years. This chart was recently generated by ERAI to show how much counterfeit part reporting has risen in the past ten years – in fact, it's increased almost tenfold since 2003, to almost 100 reports per month.



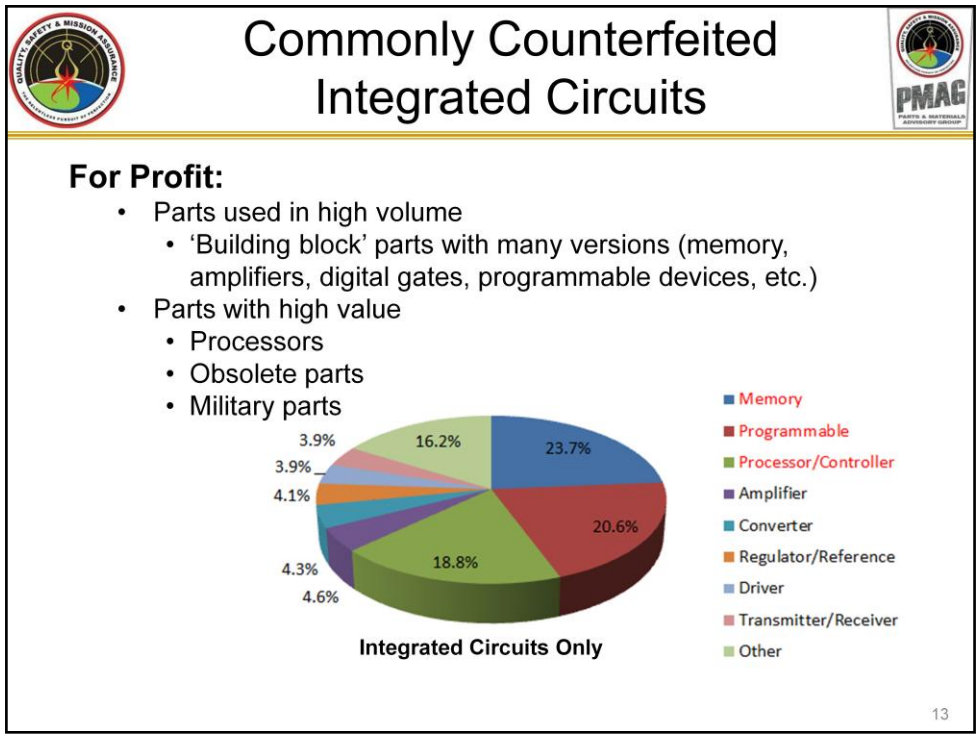
There are many different types of electronic parts, in many shapes and sizes. Prices range from less than a penny to thousands of dollars each. Some parts are readily available from trusted sources, and others are very difficult to find. Electronic parts include integrated circuits, or IC's, transistors, diodes, resistors, capacitors, inductors, relays, connectors, displays, and many other part types.

The pie chart was compiled from a listing of over 1,000 suspect counterfeit parts reported to ERAI in 2012. The data shows the majority of these parts, over five out of every six counterfeited electronic parts, are integrated circuits.



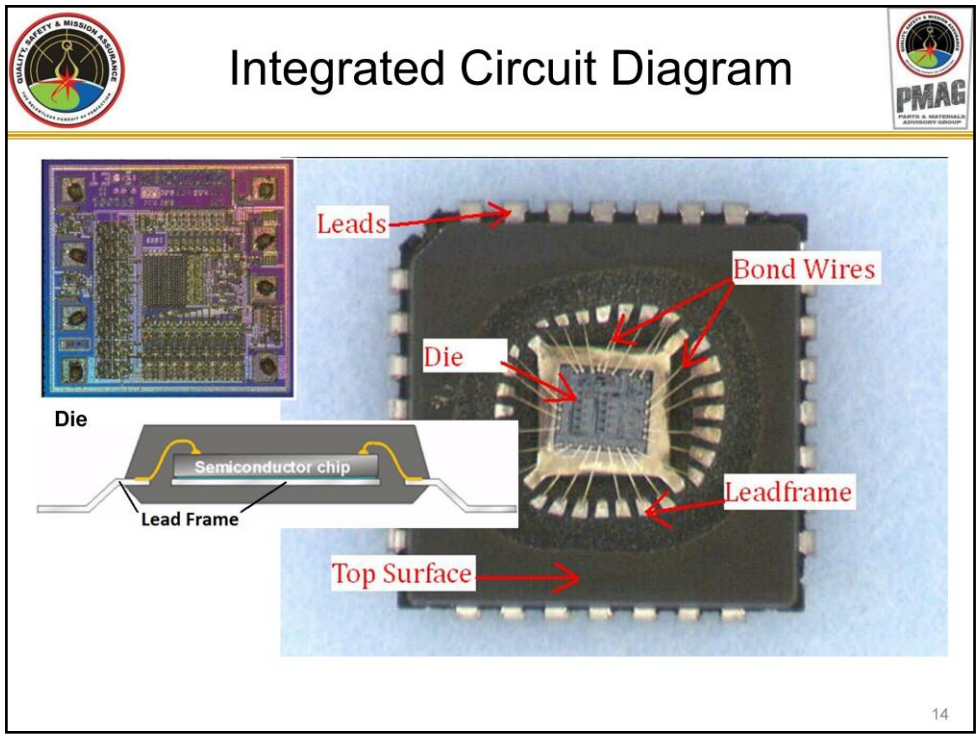
Active parts are those parts which contain semiconductor devices. Semiconductors are the building blocks of our most complex electronic circuits, like processors, amplifiers, and memory chips. Transistors, diodes, and integrated circuits, or IC's, are the most common active electronic parts. In fact, IC's are made from hundreds, thousands, or even millions of tiny transistors and diodes, connected together with other tiny parts to make a complex circuit. The data shows that about 95 percent of the counterfeited electronic parts are active parts.

Most other electronic devices, like capacitors, resistors, inductors, relays, and connectors, are considered passive parts.



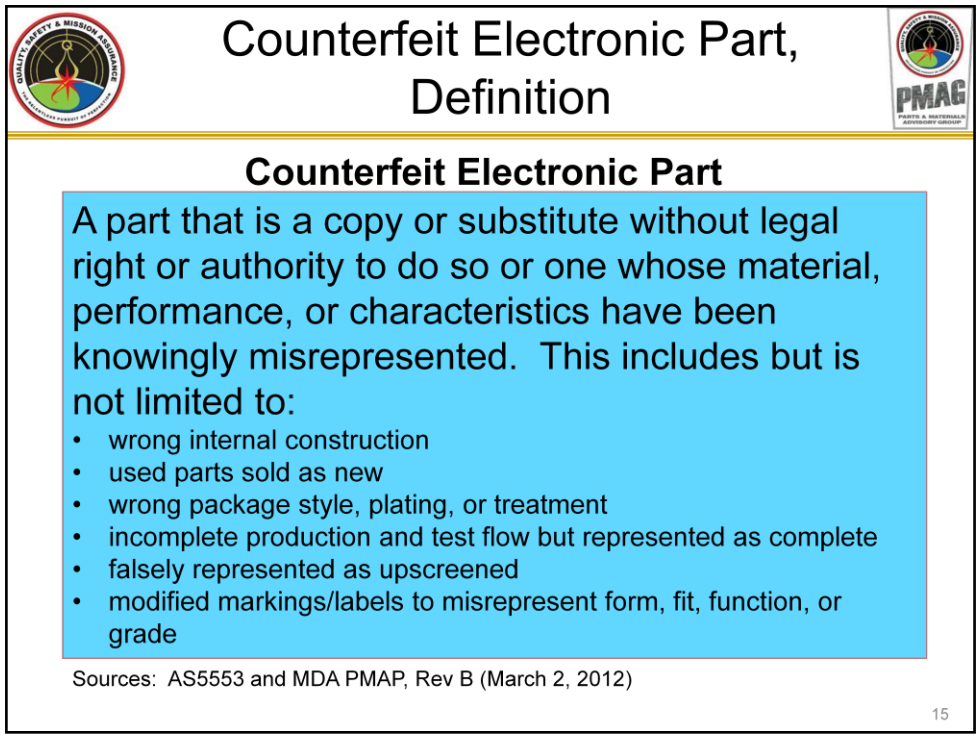
Practically any electronic part is susceptible to being counterfeited. However, the most likely parts to be counterfeited are integrated circuits that offer significant profit, either due to high volume or high value. Parts that have many versions at different speeds, temperatures, and capacities are prime candidates, because the counterfeiter can modify a 'low end' version to appear to be a high quality part, and sell it for significant profit. Memory devices, operational amplifiers, voltage regulators, digital gates, and programmable devices all fit this bill.

In addition, high complexity devices like processors, high reliability parts like military components, and high demand parts like obsolete parts are all excellent candidates for counterfeiting, because selling just a few parts can still be very profitable.



As mentioned on the previous slide, integrated circuits are made of tiny electronic parts, both passive and active, that are connected together to make a circuit that performs a specific function. The tiny parts are designed and produced in a very small package called a die. The outputs on the die are attached to a lead frame by very tiny wires, called bond wires. The lead frame includes the part's external connections, usually called pins or leads.

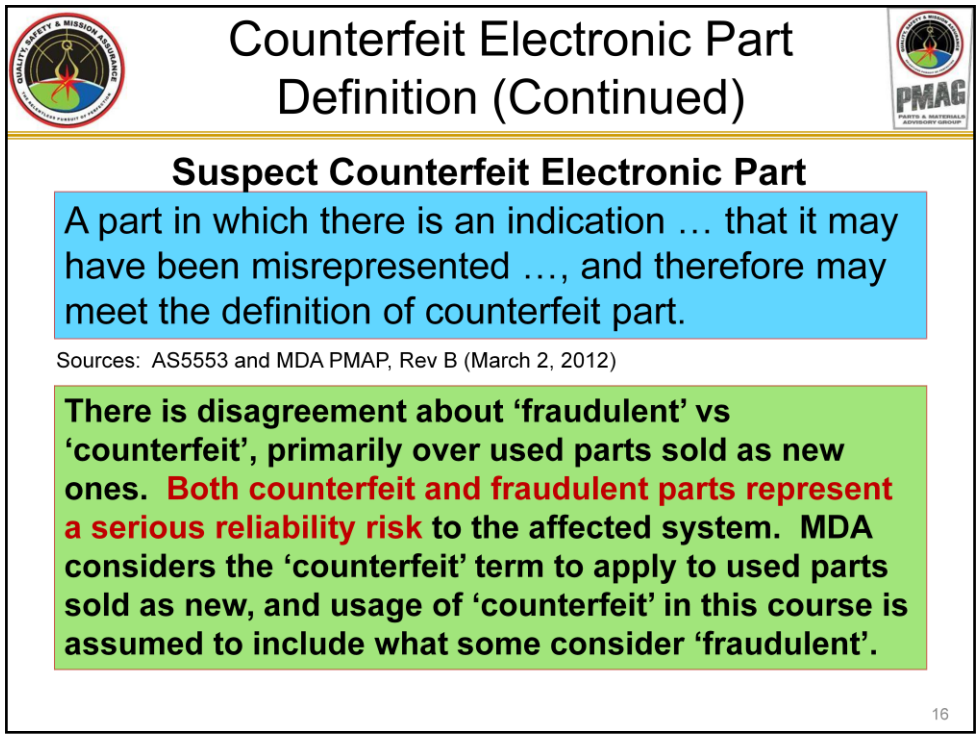
The die and bond wires are protected from damage by a protective material that covers the die and lead frame. This covering is usually made of metal or ceramic for military-grade parts, or plastic for commercial-grade parts. With the DoD efforts to utilize commercial technology, most military systems now use many plastic-encapsulated integrated circuits. These parts must be carefully assessed to ensure they will be reliable in the systems, because plastic packaging is more susceptible to moisture and temperature effects.



Counterfeit electronic parts are defined as parts illegally copied or substituted, or whose material, performance, or characteristics were knowingly misrepresented by a supplier. This includes any supplier, not just the one who sold you the parts. In other words, if a supplier unknowingly sells you counterfeit parts that were knowingly sold to him, the parts are still counterfeit.

There are hundreds of actual counterfeit electronic part examples. Some of those examples include, but are not limited to:

1. The part might be a lesser part with the wrong internal components.
2. The part might be a reclaimed or refurbished part, cleaned up to look new.
3. The part might be the wrong package style or lead plating, or it was incorrectly processed.
4. The part may have been pulled from a legitimate production line before completing all the tests, but be sold as if it has completed the processes.
5. The part might be a standard part that is misrepresented to have undergone upscreening, like vibration, radiation hardening, or extended temperature screening.
6. The part or packaging may contain false markings which misrepresent the form, fit, function, grade, manufacturer, or other parameters.



Virtually every counterfeit part is initially classified as suspect counterfeit. Usually it takes analysis of all the concerns noted during the parts' inspection and test, before the part can be classified as a counterfeit part. Ideally this should include support from the supposed manufacturer of the part.

The legal community is divided over some of the definitions of counterfeit parts. Some consider the definition of a counterfeit part not to include used parts sold as new ones, instead considering this to be fraud. MDA and the National Defense Authorization Act of 2012, Section 818, do consider these parts to be counterfeit. Therefore, throughout this course, the word 'counterfeit' describes all cases of misrepresentation of a part, including used parts sold as new ones.

Electronic Waste as a Contributing Factor

Electronic Waste (e-waste) is "discarded electrical or electronic devices. Informal processing …causes serious health and pollution problems. Some… components…contain contaminants. (Wikipedia)

"China receives 90% of the Asian recycling market"

An estimated 50 million tons of e-waste is generated yearly.

- **United States (3 million tons)**
- **China (2.3 million tons)**

Source: Basel Action Network (2002)

17

Electronic waste is thought to be the leading contributing factor for counterfeit electronic parts. Electronic waste, or e-waste, is the term which describes electronic parts and assemblies that have reached the end of their useful life. Much of this product is shipped to developing countries with cheap labor. These countries may disassemble or melt the product to retrieve valuable metals like gold, silver, and copper. Often, instead of destroying the parts for precious metals, the parts are removed, refurbished, cleaned up, and resold as new parts. This part of the commerce is illegal, and is the basis for most counterfeiting today.

It is estimated that 50 million tons of e-waste is generated every year, with the United States contributing 3 million tons, followed by China with 2.3 million tons. The recycling of this e-waste leads to serious health and pollution problems for the workers, and heavy metals and other contaminants may poison the drinking water. However, since recycling of e-waste is a very profitable industry which produces tax revenue and employs people, countries often turn a blind eye to these facts.

Electronic Waste as a Contributing Factor

Source: Basel Action Network

18

Here are some example photos of e-waste as it is received and sorted. The waste product might be computers, radios, televisions, cell phones, or any other electronic hardware. As you can see, it is handled carelessly, with little or no consideration given to maintaining the quality of the part.

Here are additional photos of e-waste products. Electronic parts are exposed to harsh weather and other environmental conditions at the recycling areas. E-Waste is often stacked and stored outside, exposed to the elements. The bottom left photo shows how different size electronic parts are separated by shaking them through a series of screens with different size openings, similar to panning for gold. The smaller parts are captured in the smaller screens, and all parts are later sorted. The bottom right photo is of a box of integrated circuits that have been removed from e-waste assemblies. Most of the IC's in the box have badly bent leads.

E-Waste Processing Effect on Quality/Reliability, Part 1

Source: SMT Corporation

Uncontrolled, careless handling of e-waste subjects parts to excess vibration and shock. Along with potential physical damage to the product, it may cause mechanical damage and compromise the integrity of the package. With cracks in the package, chemical damage can occur when contaminants cause corrosion.

20

When electronic waste is tossed around or stacked up, the assemblies are twisted and flexed, and are exposed to both vibration and shock. This can cause parts to be damaged both externally and internally. Cracks in the package can allow contaminants to reach the die, leading to corrosion and future failures. Parts that are handled this way can be damaged both mechanically and chemically. It is impossible to predict the reliability of parts that have been handled carelessly.

E-Waste Processing Effect on Quality/Reliability, Part 2

Uncontrolled heating during part removal can cause thermal damage, leading to immediate or latent failures.

Source: Basel Action Network

Source: SMT Corporation

Mishandling or sanding of parts can cause latent Electrostatic Discharge (ESD) failures or other forms of electrical damage.

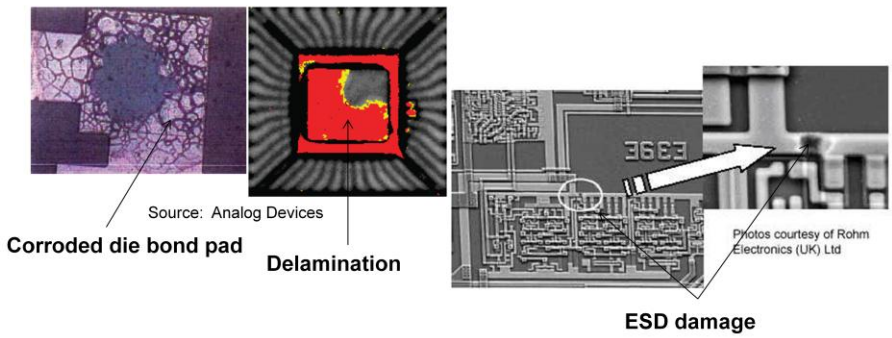
21

Additionally, the assemblies must be heated in order to melt the solder which keeps the parts attached to the board. Parts can be safely heated without being damaged – as long as the process is not too quick or too hot. However, these recycling or refurbishing operations do not use proper heating practices, as evidenced in the photograph at the bottom of this slide. Uncontrolled heating processes like this can cause thermal damage like cracks and delamination, leading to latent failures. Delamination is the separation of internal layers which can break wire bonds or allow corrosive materials to enter the part.

In addition, electrostatic discharge, or ESD, can cause electrical damage to the parts if they are handled without proper grounding. Some electronic parts can be damaged by an electrical shock of a hundred volts or less. For comparison, when you feel a zap on a doorknob after walking on carpet, you transferred at least 3,000 volts to the doorknob.

E-Waste Processing Effect on Quality/Reliability, Part 3

All of the images below are examples of damage caused by mechanical, chemical, thermal, or electrical stress.
All of them reduce reliability. None of them are visible by looking at the part's exterior.

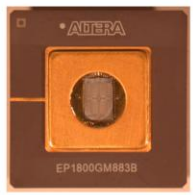


22

These images are all of electronic parts that have either failed, or are likely to fail soon. The handling, stacking, removal, and refurbishment of electronic parts and assemblies, if not closely controlled, will cause damage like this. None of the damage is readily visible on the outside of the package. Parts can be damaged mechanically, chemically, thermally, and electrically.

The 'Quality' of Counterfeiting

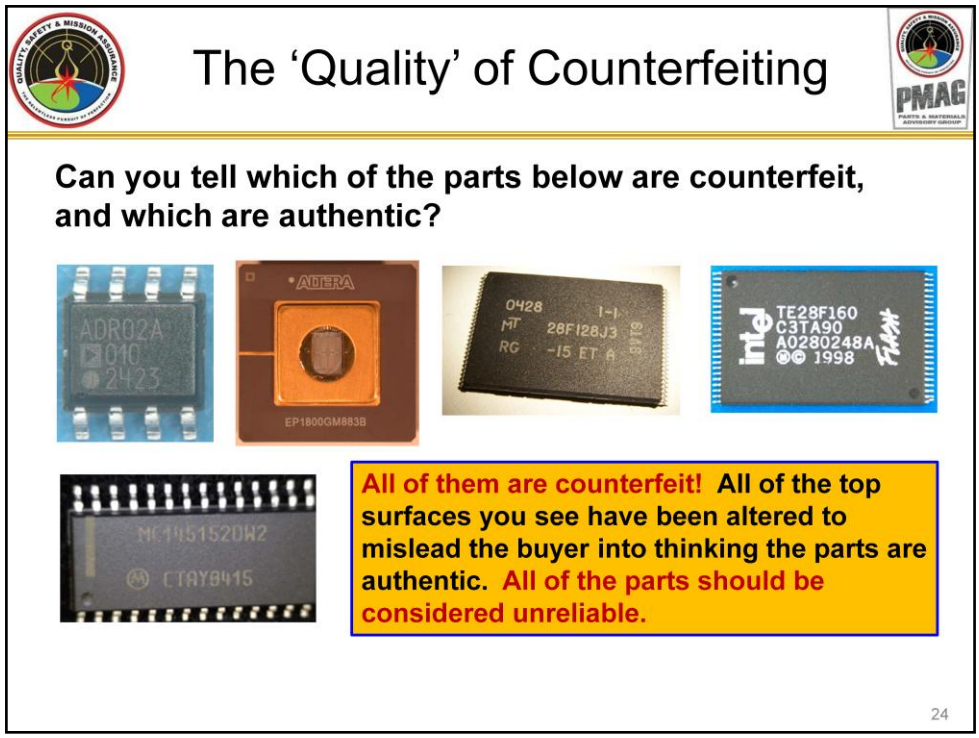
Can you tell which of the parts below are counterfeit, and which are authentic?



Hint: Look for visual indicators like logos, cracks, smears, or other signs of alteration.

23

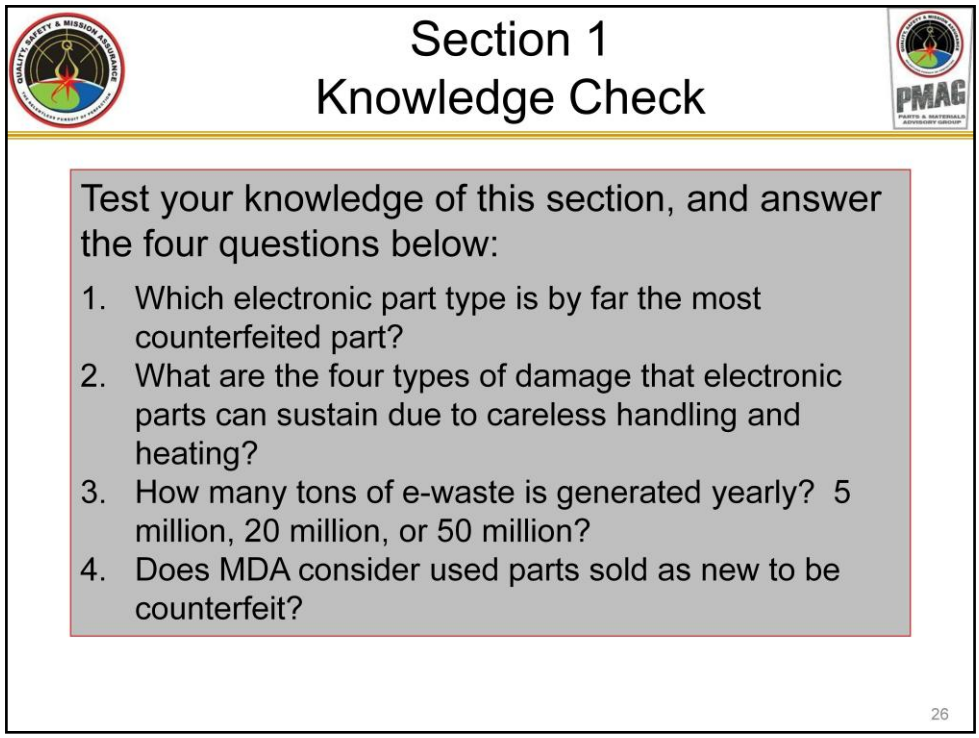
Look at the photos and try to detect which of the parts are counterfeit, and which ones are authentic. Can you tell the difference? The answers are on the next slide.



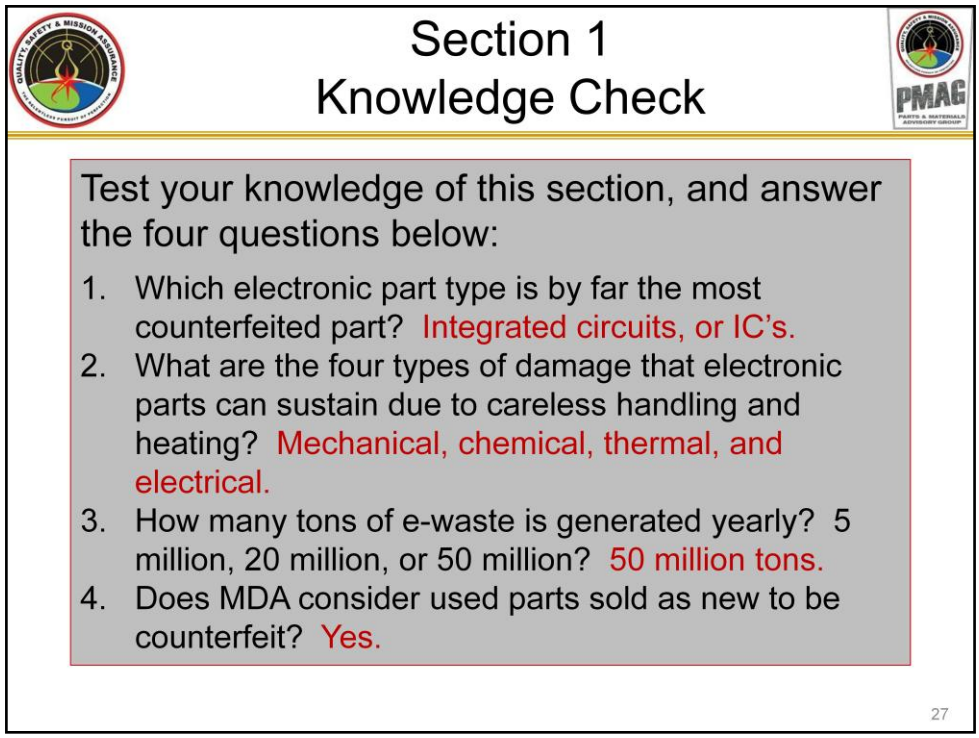
All of the parts in the photos are counterfeit, with altered or sanded top surfaces. You might have seen photos of badly counterfeited parts - misspelled words, uneven markings, obvious recoatings, etc. Don't consider these images typical counterfeit parts. Today's counterfeit parts are not poorly-modified parts that you can expect to fail the first time they are tested. They are usually carefully-modified parts that have been specially selected for a high probability of passing visual inspection and electrical test.

However, the parts should still be considered potentially unreliable, regardless of the test results. Just because a counterfeit part passes all of the electrical tests today, does not mean it won't fail tomorrow or the next day, when the system may be needed to save lives.

There are also numerous non-electronic parts or electronic assemblies that have been counterfeited. This slide shows a few of the recent examples. Moving clockwise from the top left, Cisco interface cards have been found with duplicate serial numbers and many used parts, including inductors, connectors, and labels. Bolts with improper heat treatment or insufficient strength are also common. Smoke detectors were sold in Atlanta that contained counterfeit Underwriters Laboratory labels, and were of extremely poor quality – some would not even function. Mixing and mislabeling of refrigerants has resulted in explosions and deaths. And counterfeit fire extinguishers dispense flour or sawdust instead of flame retardants. These are just a few examples of counterfeit material that is not an electronic part.



Test your knowledge of this section by reading each of the four questions. What is your answer for each one? Go to the next slide to see how you did.

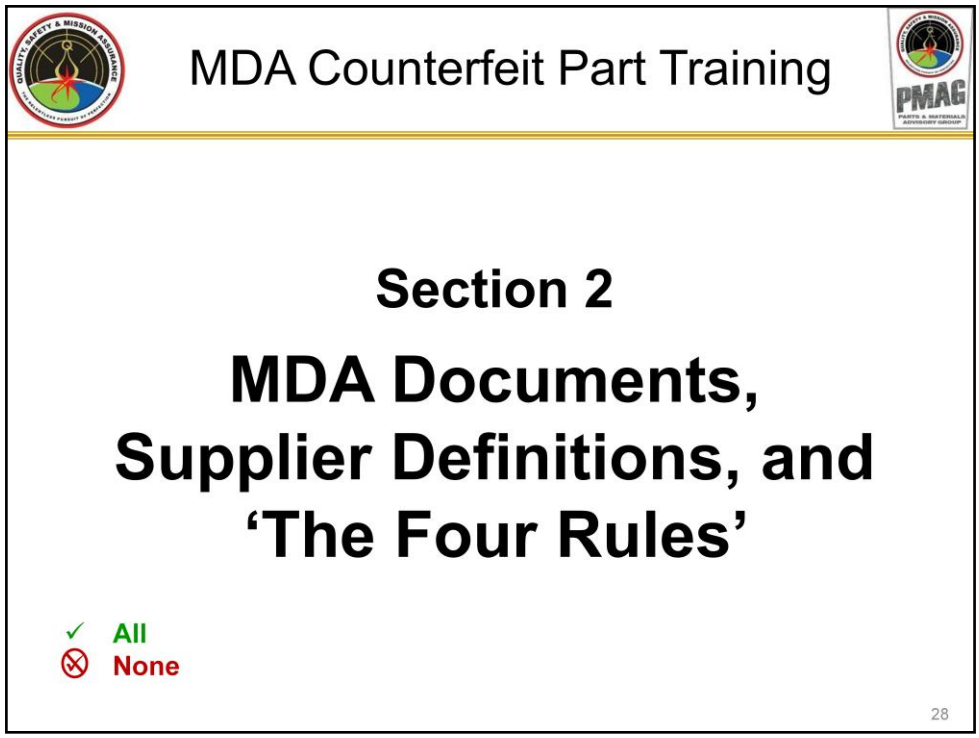


Integrated circuits are the most commonly counterfeited electronic parts. Perhaps 85 percent of all counterfeit electronic parts are IC's.

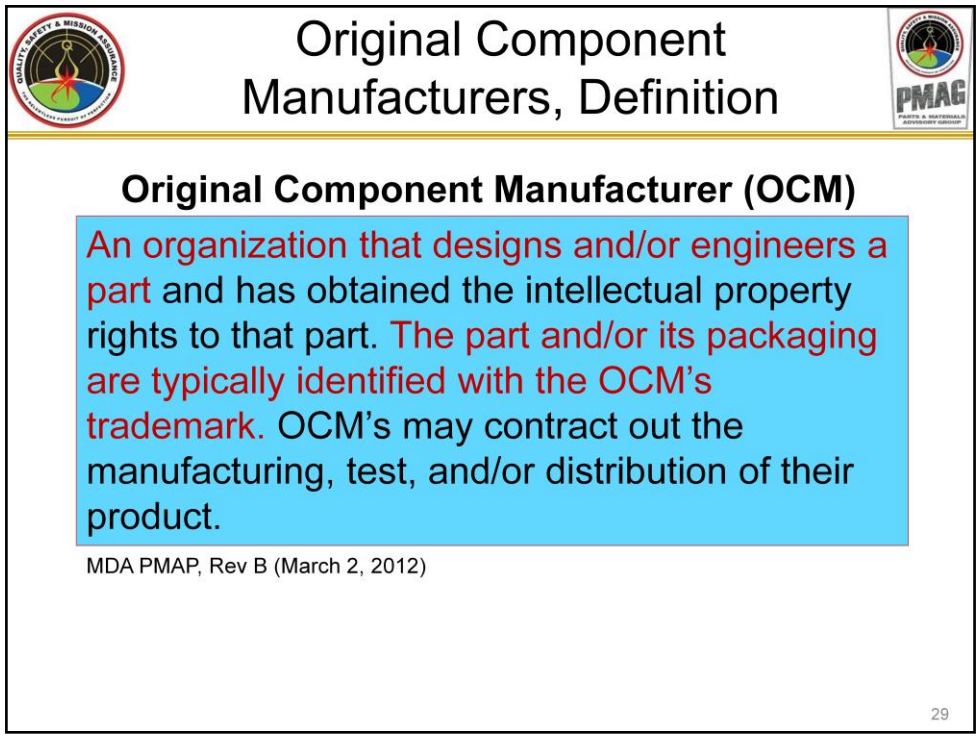
Badly controlled handling, alteration, or refurbishment of electronic parts can result in mechanical, chemical, thermal, and electrical damage. Usually this damage is difficult or impossible to detect by just inspecting the part's exterior.

It is estimated that the world generates 50 million tons of electronic waste every year, with much of it being shipped to developing countries for reclamation.

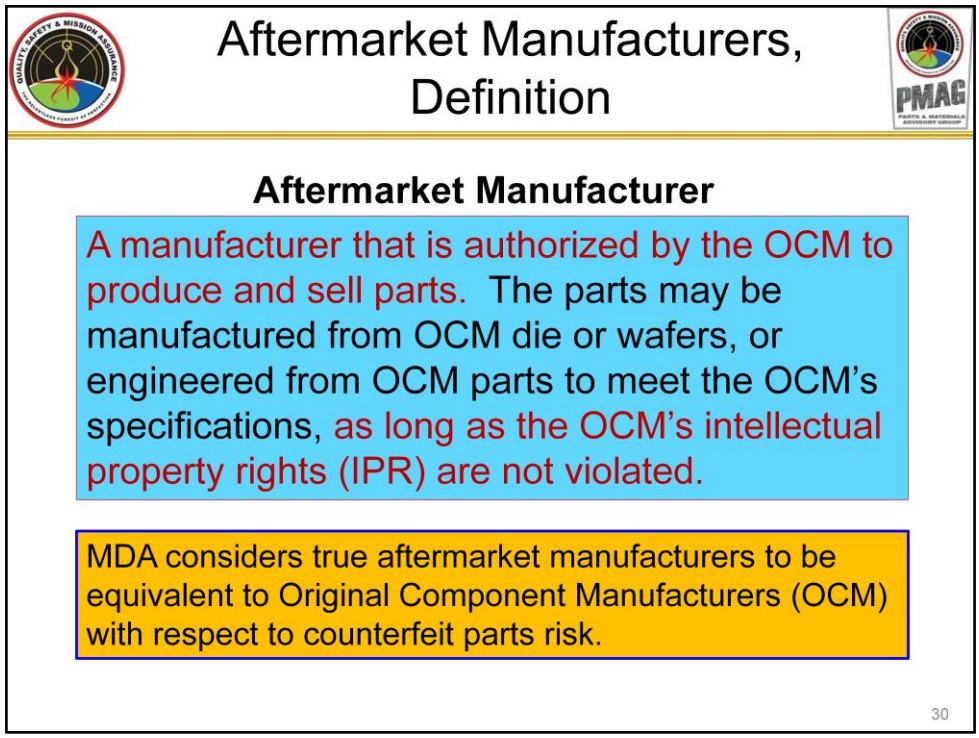
MDA does consider used parts sold as new ones to be counterfeit.



In this section you will briefly learn about the different types of electronic part suppliers, and why some are less risky than others with respect to the counterfeit parts risk. You will also learn the four basic rules for keeping counterfeit electronic parts out of MDA hardware.

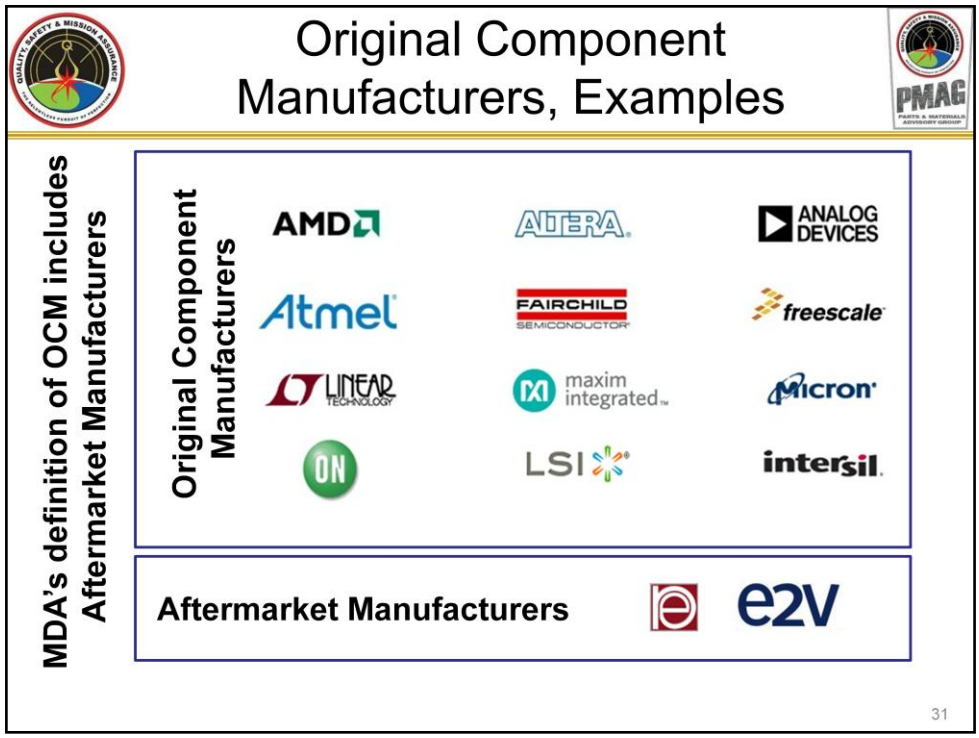


Let's start with some supplier definitions. Original Component Manufacturers, or OCMs, are the companies that design and own the intellectual property rights for an electronic part. OCMs warrant the quality and reliability of the parts through extensive analysis, test, and processing controls, and attach the company logo or trademark to the documentation, and often the part itself.



Aftermarket manufacturers are companies that produce parts equivalent to an OCM's parts, with OCM permission. This usually happens when a part is discontinued, but is still in demand. The aftermarket manufacturer may purchase wafers, die, tooling, or intellectual property rights for the part, so that equivalent parts can be manufactured to supply the market. The parts typically have the aftermarket manufacturer's logo, but are advertised as replacement parts. The key to aftermarket manufacturers being considered legitimate is the authorization from the OCM to produce the parts.

MDA considers the risk of buying parts from aftermarket manufacturers to be no greater than buying from OCM's.

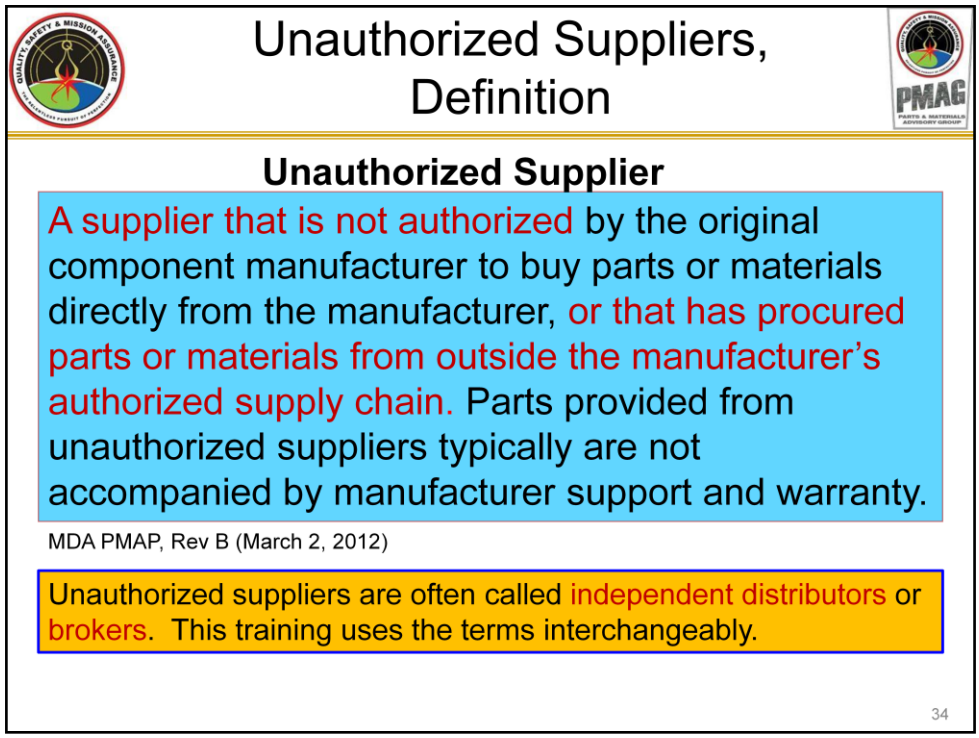


Here are several examples of companies that meet the definition of an original component manufacturer. These companies make electronic parts under their own brand name and trademark. This includes aftermarket manufacturers like Rochester Electronics and E2V, who buy the rights to manufacture replacement parts, and sell them under their own trademark.

Authorized suppliers have contractual agreements with original component manufacturers which allow the companies to buy electronic parts directly from the manufacturer. Because these companies are audited and verified by the OCMs to handle, track, and ship parts in compliance with the OCM's requirements, the parts can be sold with full manufacturer's support and warranty. Authorized suppliers generally are referred to as authorized or franchised distributors. The two terms are interchangeable. Buying parts from an authorized supplier is the next best thing to buying the parts directly from the OCM.

Companies like Arrow, Avnet, Future, and several others are examples of authorized suppliers. There are many additional authorized suppliers not listed here. All of these companies should be considered good sources for authentic electronic parts.

However, it is important to understand that no single company is authorized to sell parts from every electronics manufacturer. If any company sells parts without being authorized by the OCM to sell those parts, that company is not an authorized supplier for that sale.



It's time to learn what an unauthorized supplier is, because this type of supplier is the source of over 99 percent of all counterfeit electronic parts. Unauthorized suppliers do not make their own electronic parts. Instead, they buy them from a supplier and sell them to a customer. They might buy the parts from any number of supplier types, including other unauthorized suppliers. Unauthorized suppliers do not usually have contractual agreements with original component manufacturers, or OCMs. Therefore, an unauthorized supplier cannot usually offer a full manufacturer's warranty for parts sold. Unauthorized suppliers are often referred to as independent distributors, non-franchised distributors, or brokers. This training uses the terms interchangeably.

A purchaser can't always determine the size and capability of an independent distributor by checking out the website. Small or limited-capability independent distributors can mask their size and limitations by boasting very large line cards, or OCM listings, exaggerating test capabilities, using commercial shipping locations to mask a residential business, and in the case of Company B, even inserting a photograph of someone else's business in order to look more 'corporate'.

The two examples here are actual U.S.-based independent distributors that were residential businesses in 2009 when MDA contacted them. The quotes in red extracted from the websites imply the companies are large businesses with significant capabilities. Actually, the majority of independent distributors are very small companies, with 10 or fewer employees. In 2010 a sampling of ERAI's member addresses indicated that over 10 percent of the companies conducted business from a house. And this does not count companies which used commercial mail facilities, like a UPS Store, to mask their true location.

Where Do Unauthorized Suppliers Get Their Parts?

OCMs and Authorized Suppliers

- Only if parts are available

OEMs* and Contract Manufacturers

- Excess stock no longer needed

Other Unauthorized Suppliers

- Independent distributors
- Brokers
- May be from high-risk foreign countries (these are usually the cheapest parts)

Highest Risk

* MDA considers OEMs (Original Equipment Manufacturers) to be organizations that build assemblies (Dell, Cisco, etc.) from discrete parts. This does not include OCMs, which are companies that design and/or manufacturer parts.

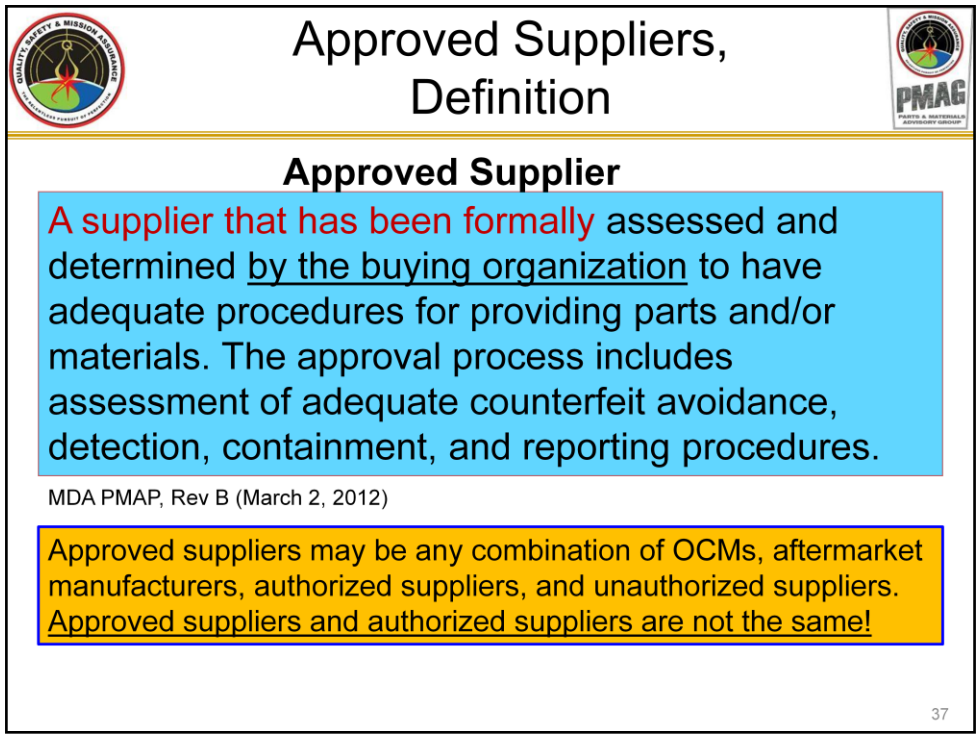
36

Unauthorized suppliers are tasked with finding electronic parts for their customers. The parts are found primarily from three sources.

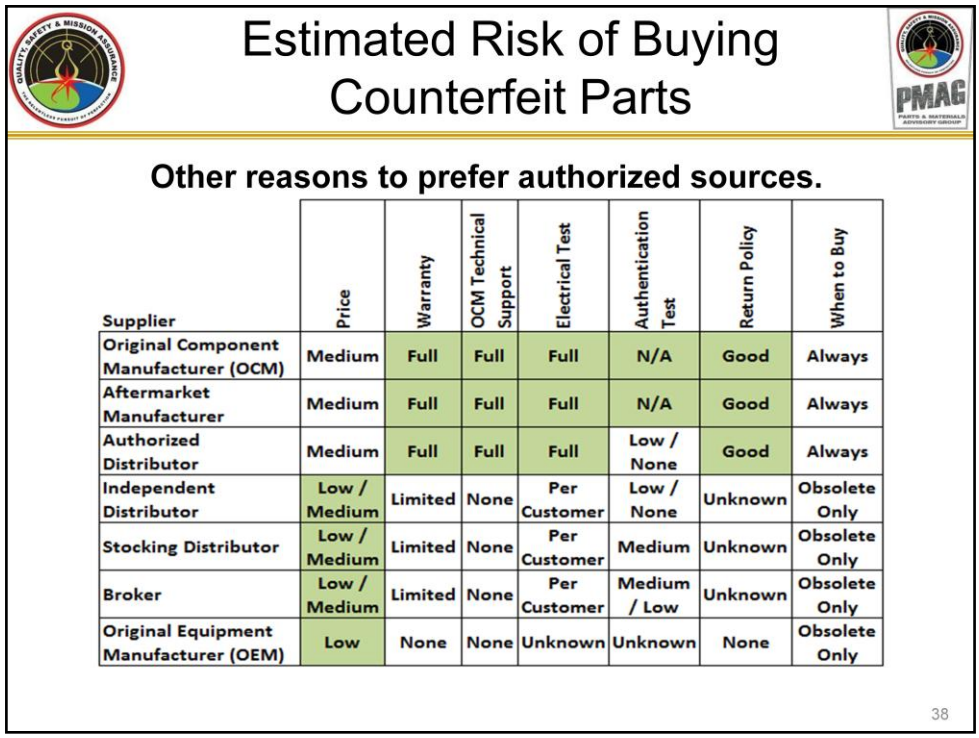
1. If the parts are not out of production, OCMs and authorized suppliers often have parts available, although many OCMs will not sell electronic parts directly to an unauthorized supplier such as an independent distributor.

2. Original equipment manufacturers, or OEMs, contractors, and contract manufacturers often sell excess parts, if the parts are no longer needed. This is an important source of supply for unauthorized suppliers, who bid against other unauthorized suppliers for the parts, usually in large mixed lots. The photo is an example lot that an independent distributor 'won' from a large defense contractor. The parts usually are missing traceability to the supplier, and as seen here, may be packed haphazardly.

3. Most of an unauthorized supplier's parts are bought from other unauthorized suppliers. It is common for an independent distributor to have hundreds, if not thousands of approved suppliers to refer to, as well as maintain memberships in several internet-based search engines for finding electronic parts. By this method, even the smallest independent distributor can appear to be well-connected and have access to millions of parts and a large warehouse, even if the actual business is a den in the owner's house. Unless an unauthorized supplier is very concerned about the counterfeit parts risk, and is determined to only use similarly concerned suppliers, it will almost certainly buy counterfeit electronic parts from time to time.

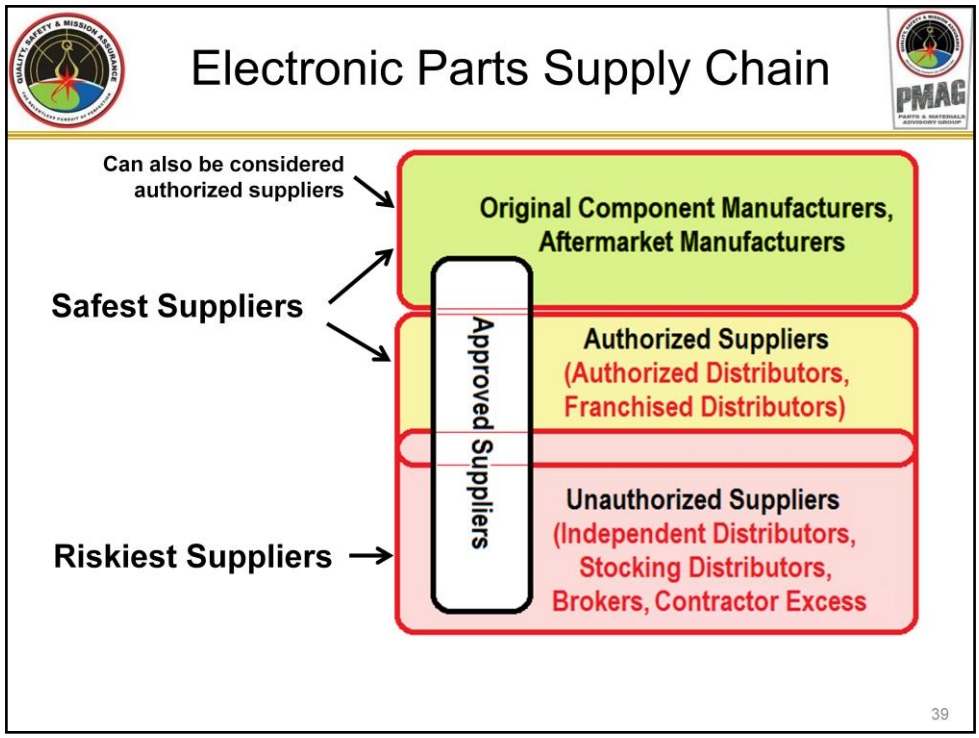


Approved suppliers can be OCM's, aftermarket manufacturers, authorized suppliers, and unauthorized suppliers. These are companies that have been assessed by a potential customer – for example an MDA contractor - and have been approved by that customer to provide parts or materials. Do not confuse an approved supplier with an authorized supplier!



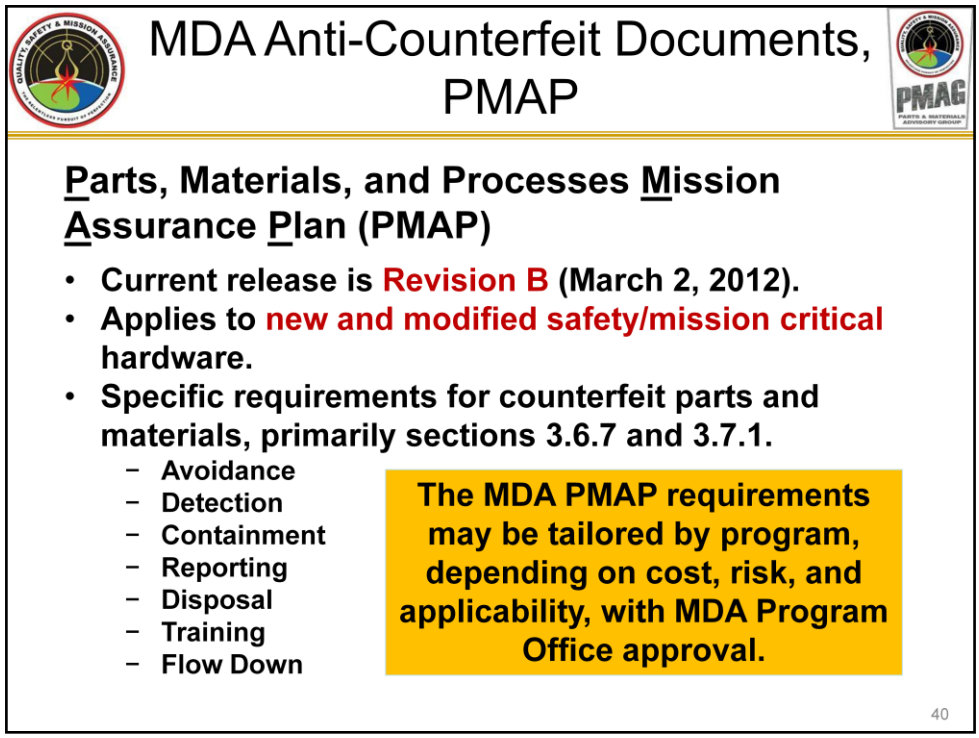
Supplier	Price	Warranty	OCM Technical Support	Electrical Test	Authentication Test	Return Policy	When to Buy
Original Component Manufacturer (OCM)	Medium	Full	Full	Full	N/A	Good	Always
Aftermarket Manufacturer	Medium	Full	Full	Full	N/A	Good	Always
Authorized Distributor	Medium	Full	Full	Full	Low / None	Good	Always
Independent Distributor	Low / Medium	Limited	None	Per Customer	Low / None	Unknown	Obsolete Only
Stocking Distributor	Low / Medium	Limited	None	Per Customer	Medium	Unknown	Obsolete Only
Broker	Low / Medium	Limited	None	Per Customer	Medium / Low	Unknown	Obsolete Only
Original Equipment Manufacturer (OEM)	Low	None	None	Unknown	Unknown	None	Obsolete Only

There are plenty of reasons to buy from an OCM or authorized supplier. This chart lists several of them. While parts bought from authorized suppliers might be more expensive, there are reasons for this. With parts bought from the authorized supply chain, the OCM will provide warranty and technical support. The part lot has also undergone testing to the data sheet, and the parts have been handled in accordance with industry standards. Not all of these 'pluses' relate to counterfeit parts avoidance, but they do contribute to the customer having reliable parts, backed by the manufacturer.



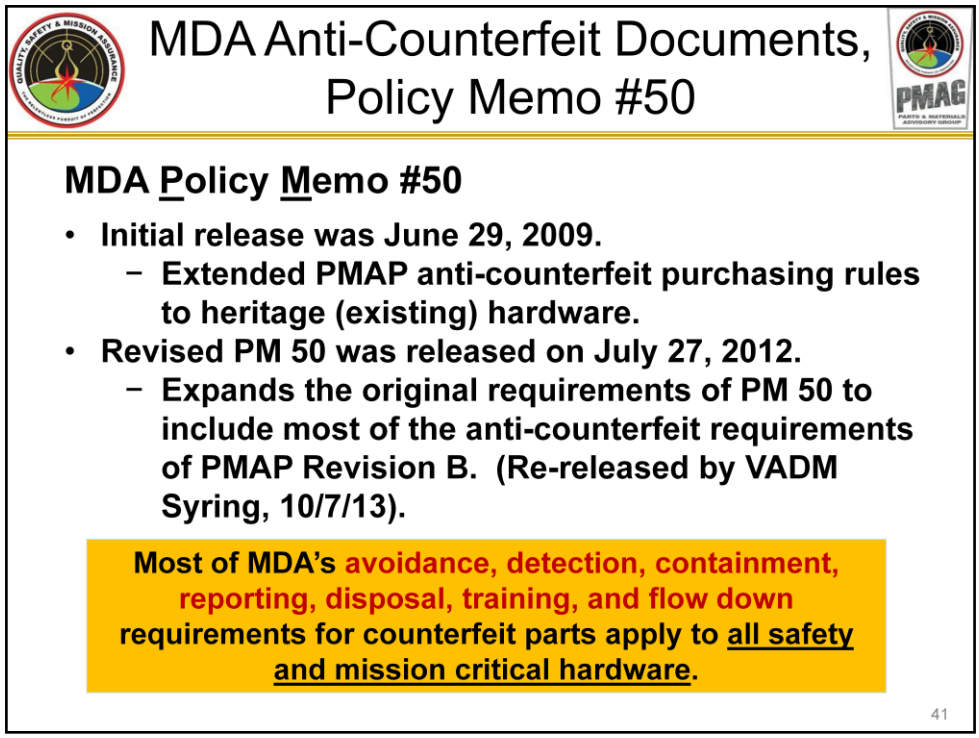
This illustrates the supply chain risk for counterfeit parts. Original component manufacturers are the only organizations in the supply chain that can be considered completely safe to sell authentic parts. However, the OCM's authorized suppliers can also be considered a very low risk. Unauthorized suppliers like independent distributors, stocking distributors, and brokers, should always be considered risky. Even excess parts that contractors sell should be considered risky. Approved suppliers can be in any of the three supplier type categories.

Purchases from unauthorized suppliers can be mitigated in several ways, which will be discussed in later sections.



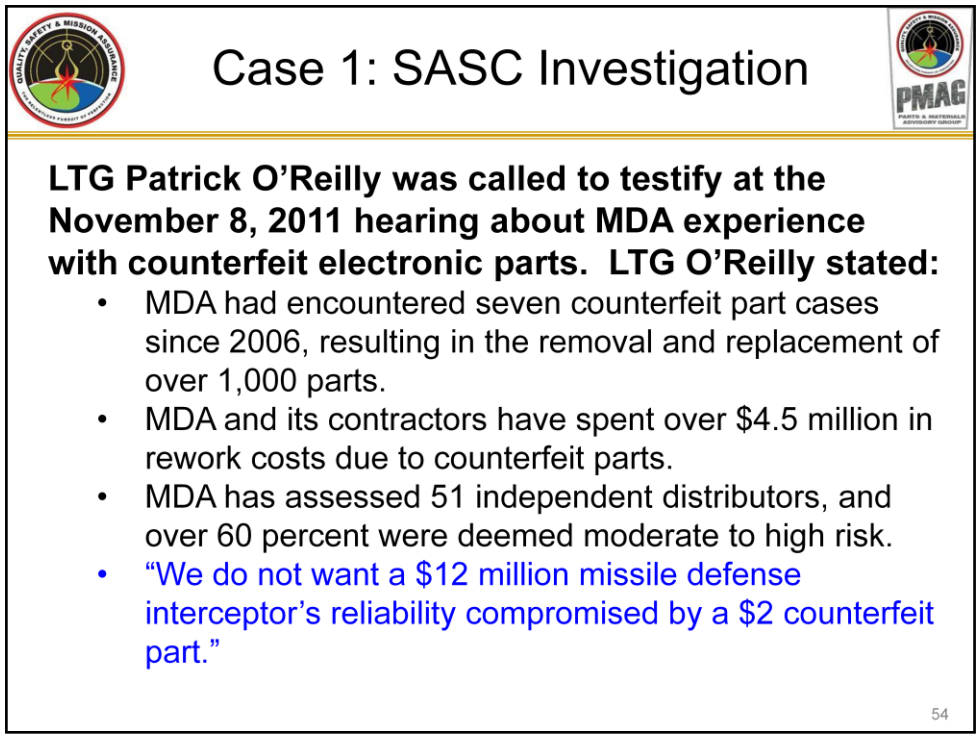
MDA has two core requirements documents for counterfeit parts and materials. The first one is the Parts, Materials, and Processes Mission Assurance Plan, or PMAP (pronounced 'PEE-map'). The PMAP establishes guidance and requirements for new and modified safety and mission critical hardware. Revision B was released in March 2012. The PMAP's anti-counterfeit requirements are primarily listed in sections 3.6.7, Counterfeit Parts and Materials, and 3.7.1, Supplier/Vendor Selection and Surveillance, although there are anti-counterfeit requirements scattered throughout the document. The requirements govern avoidance, detection, containment, reporting, and disposal of counterfeit parts and materials, as well as training and flow down.

The PMAP is the basis for all prime contractor Parts, Materials, and Processes, or PMP plans. As the document is flowed down through MDA's supply chain, it may be tailored as justified by cost, risk, and applicability, with MDA Program Office approval. The actual requirements will flow from each subcontractor's direct customer.



MDA's Policy Memo #50 was released in 2009 to apply a few of the PMAP's core purchasing requirements to heritage mission and safety critical hardware. With the release of Revision B of the PMAP in 2012, Policy Memo #50 was revised as well. The new revision applies most of the requirements of PMAP sections 3.6.7 and 3.7.1 to heritage hardware.

When MDA requirements are discussed in a later section, there will be a designation to indicate whether the requirements apply to only new and modified critical, or to all critical hardware.



MDA's leader, Lieutenant General Patrick O'Reilly, also testified at the hearing at SASC request. MDA was viewed in a positive light by the investigators for their proactive efforts to combat counterfeit electronic parts, and for Lieutenant General O'Reilly's tough stance on the reliability of counterfeit parts. At the hearing Lieutenant General O'Reilly disclosed that MDA had already had seven known counterfeit part incidents, which had resulted in the removal and replacement of over 1,000 parts. He listed $4.5 million as the rework/repair costs, shared by MDA and its contractors. Lieutenant General O'Reilly also indicated that MDA on-site assessments of American independent distributors had found over 60 percent of them with at least a moderate risk of selling counterfeit electronic parts. The general's closing statement was that "we do not want a $12 million missile defense interceptor's reliability compromised by a $2 counterfeit part".

Case 2: Internet Search Engines

Case information removed – not for public use.

55

Case 3: Buy American?

Case information removed – not for public use. Summary, foreign-made counterfeit parts are often bought from US-based unauthorized suppliers.

Case 4: American Accomplices

VisionTech (Independent Distributor)

- Located in the Tampa, FL, area.
- Raided in 2010, convicted in 2011.
- Imported and sold over $15 million in counterfeits from 2007 to 2009.
- Almost all product was counterfeit.
- 867 domestic customers.

tim@visiontechc Rose(F) 1st-IC going to need better ink
tim@visiontechc Rose(F) 1st-IC our customers are beginning to use acetone on all parts
Rose(F) 1st-IC tim@visiontechc OK. then price is higher. some is double.
tim@visiontechc Rose(F) 1st-IC can you tell suppliers neec parts that ink doesnt come off from now on

Fight RMA's Test Report / Act Surprised

ELECTROSTATIC STICKER HAD SPELLING ERROR ON IT YEEK IT OFF

Data was extracted from publicly available Criminal Case 10-245 (PLF), released September 9, 2011.
https://www.yumpu.com/en/document/view/17897065/united-states-district-court-for-the-cox-media-group/5

57

In 2010, investigators raided VisionTech, an independent distributor in Florida that knowingly sold counterfeit electronic parts to 867 different U.S-based customers, most of them independent distributors. The company had a commercial address and a professional website, yet almost all of the product they sold to their customers was remarked counterfeit product bought from Chinese suppliers. Millions of counterfeit parts were likely sold between 2007 and 2010. The yellow highlighted excerpts were found by investigators in VisionTech's records, and proves the company knew the parts were counterfeit. VisionTech told their suppliers to use better remarking inks, instructed their employees to act surprised when their customers reported failures, and removed labels that might cause suspicion.

Case 4: American Accomplices

MVP Micro (Independent Distributor)

- Located in the Los Angeles area.
- Raided in 2009, convicted in 2012.
- Seven alias companies.
- Sent parts and die out for remarking and re-production.
- 302 Domestic customers.

Hello Michael,

I need a quote on some parts to be remarked.

Parts that are going to be remarked PN: SCC28C94C1N will be remarked to show PN: SC26C94A1N

I've attached a picture to show the format of how I want the parts to be remarked.

All I want to change in this remark is the part number only!

Everything else will remain the same: the LC, DC, and Philips logo remain the same.

Data was extracted from publicly available Criminal Case 09-cr-00208-EGS, released December 13, 2011.
https://www.yumpu.com/en/document/view/17897065/united-states-district-court-for-the-cox-media-group/5

58

Here is another example. MVP Micro, an independent distributor in the Los Angeles area, sold electronic parts to 302 different U.S-based customers, most of them independent distributors. The company sold parts under at least seven different independent distributor aliases, each with its own professional website. MVP Micro sent parts to another company for remarking, and was also removing the internal die from used or scrap electronic parts for repackaging as more expensive parts.

Case 4: American Accomplices

MVP Micro, continued

Personnel salvaged die from product to be rebuilt as new (not remarked) product. One example:

- ICM7170IPG Harris/Intersil IC, bought for pennies.
- Part die was removed and shipped overseas.
- Repackaged as ICM7170AIBG (smaller better part).
- Hundreds of parts salvaged in one shift by one person.
- Parts were resold for around $38.

The new part contains:

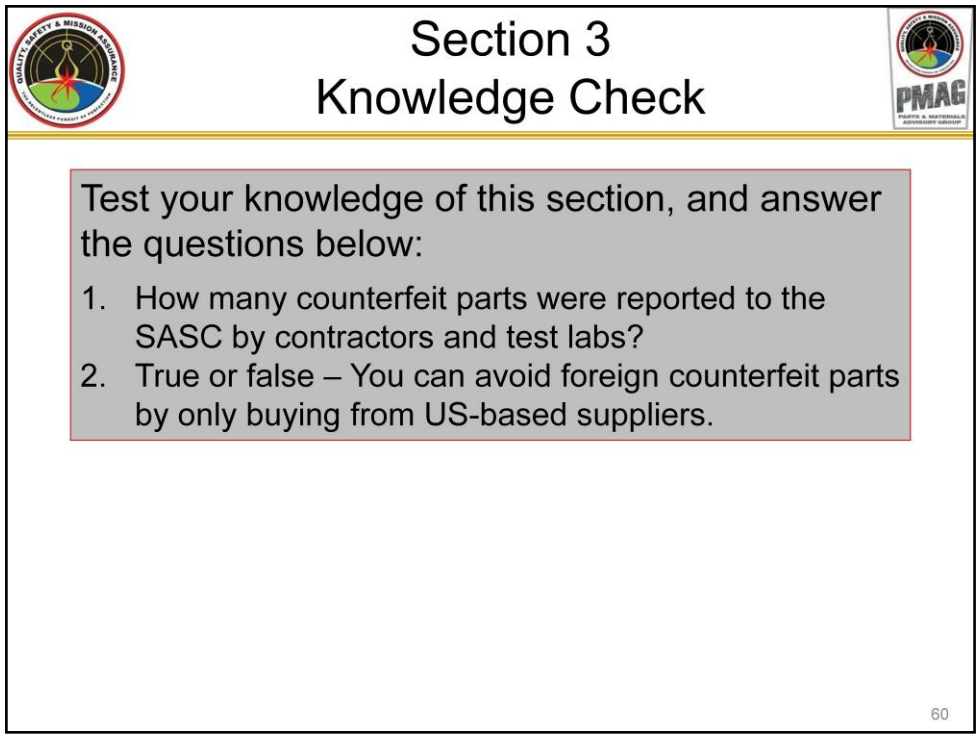
- Used die.
- Chemical, thermal, electrical, or mechanical damage?

Source: American Electronics Resource, Inc. (AERI)

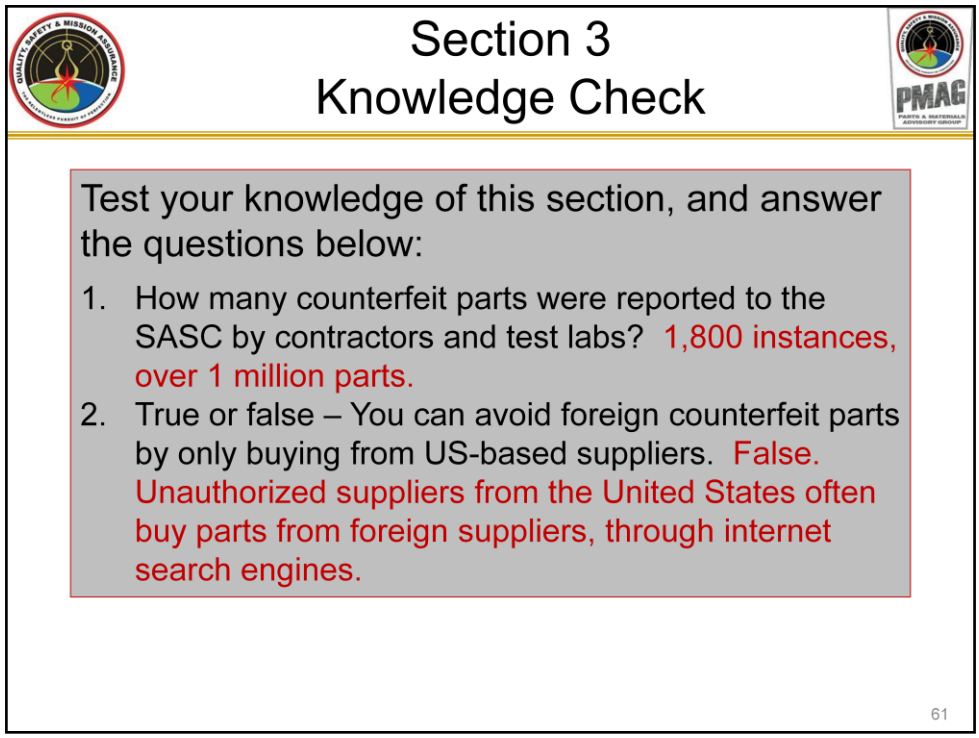
59

Here's a die removal story shared by a former MVP Micro employee. The ICM7170IPG part is an integrated circuit that is apparently readily available at cheap prices. Employees would remove the die using acid – which can cause chemical damage, heat – which can cause thermal damage, and a razor knife – which can cause mechanical damage. The parts would be sent overseas to be installed into a brand new package, and sent back as a counterfeit ICM7170AIBG part, a smaller but more expensive part. MVP Micro could make hundreds of thousands of dollars doing this at high volume.

In this particular case, the issue would be very difficult for the customer to detect. The package is brand new, with no remarking. The pins or leads are also new. The die is authentic. The 'new' part is in a smaller package, and is marked as if it's a better part. The only sure way to detect the crime without destroying parts would be if the external markings were poor quality, if the part was tested to the complete electrical parameters, or if the die was sufficiently damaged to cause immediate test failures. Barring these possibilities, the customer would unknowingly be placing used, unreliable parts into his system.

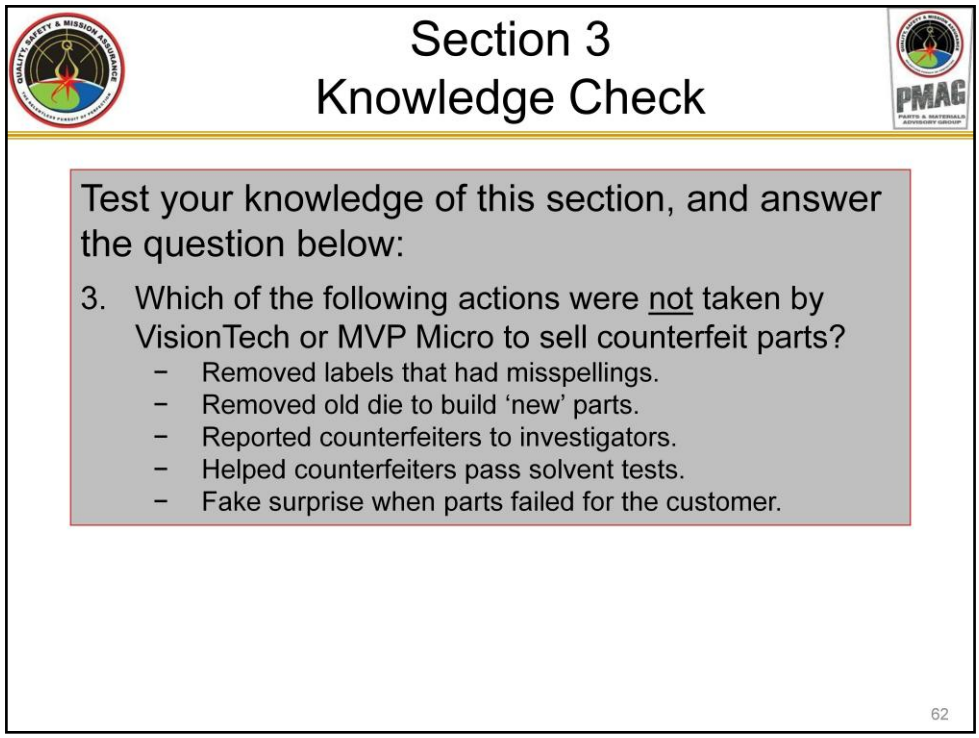


Test your knowledge of this section by reading each of the upcoming three questions. What is your answer for each one? Go to the next slides to see how you did.

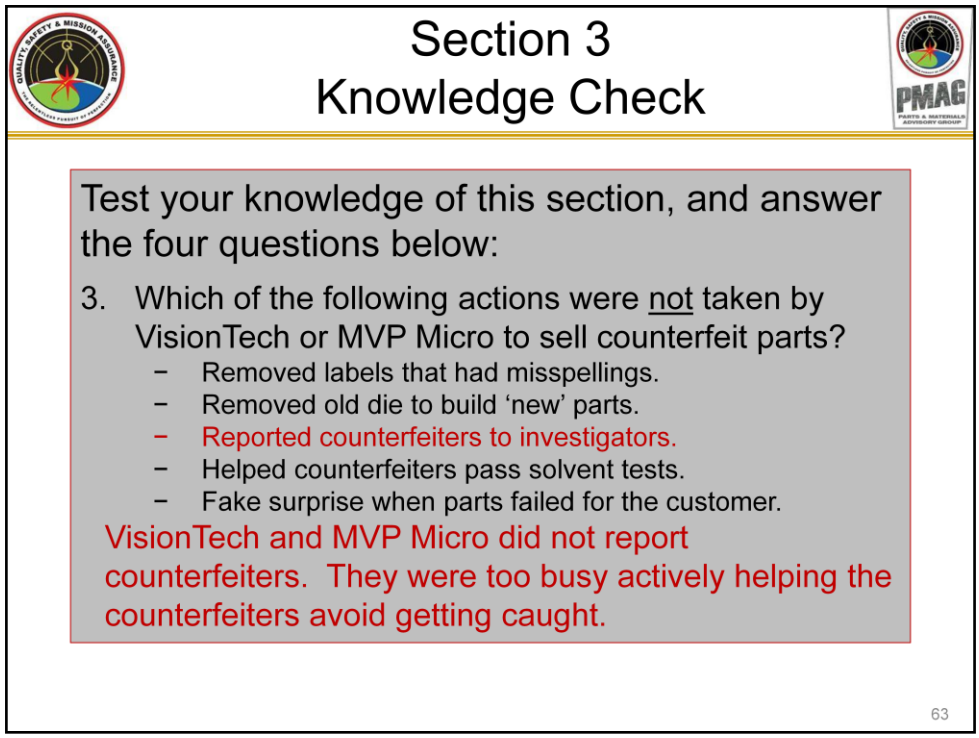


For question #1, contractors and test labs reported 1,800 cases of counterfeit parts to the Senate Armed Services Committee, totaling over one million parts. The reports covered a two-year span.

Question #2 is false – because of internet trading platforms and sophisticated search engines, US-based independent distributors can readily find and purchase parts from all over the world. And they often do.

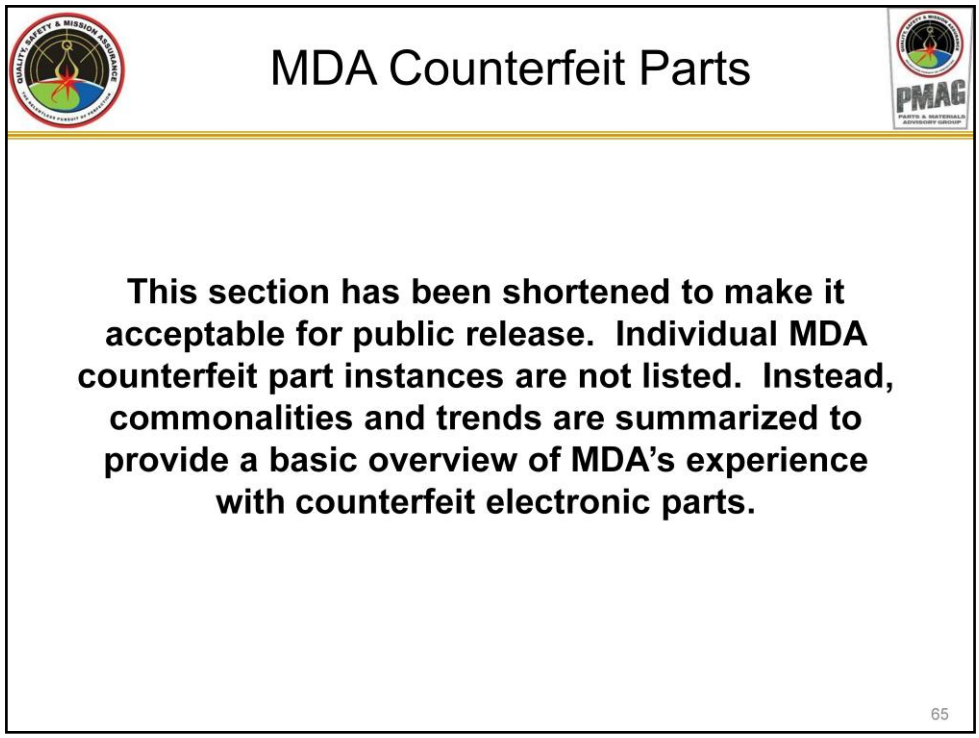


Here is the third question.

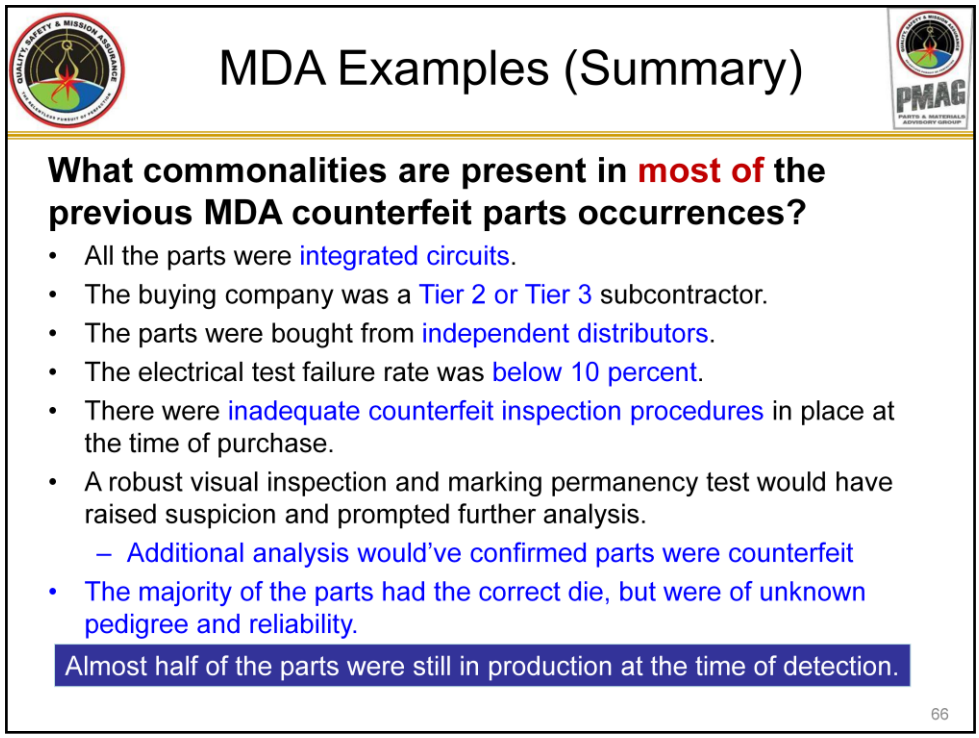


VisionTech and MVP Micro took many actions to disguise their efforts to sell counterfeit electronic parts. In fact, the only thing on the list they didn't do was report the counterfeiters to investigators.

In this section you will find out about MDA's firsthand experience with counterfeit electronic parts. This is the only section in this training that is considered 'For Official Use Only'.



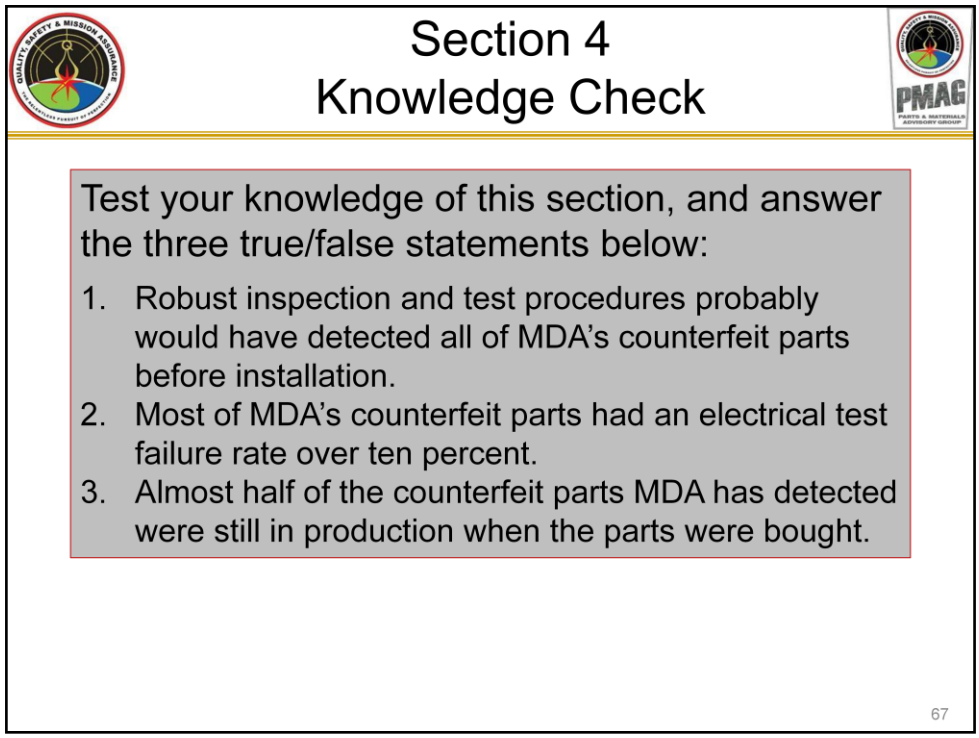
This section has been shortened to make it acceptable for public release. Individual MDA counterfeit part instances are not listed. Instead, commonalities and trends are summarized to provide a basic overview of MDA's experience with counterfeit electronic parts.



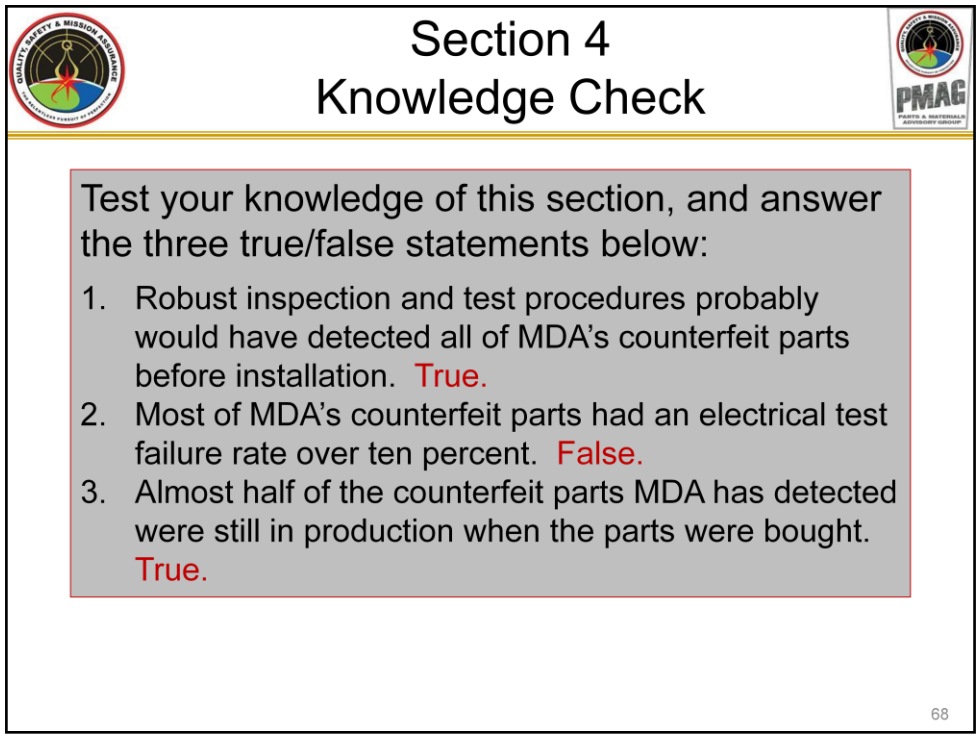
Here are the common points from the MDA counterfeit part events:

1. All of the parts were integrated circuits.
2. All of the parts were bought from independent distributors, by a Tier 2 or 3 subcontractor.
3. The electrical test failure rate of most of the parts was below ten percent.
4. Proper inspection and chemical tests would've detected the parts, if they were tailored to counterfeit parts detection.
5. The majority of the parts had the correct die, and even the parts with incorrect die had a limited failure rate.

Almost half of the counterfeit parts were still in production at the time of detection, and therefore could have been bought from authorized suppliers.



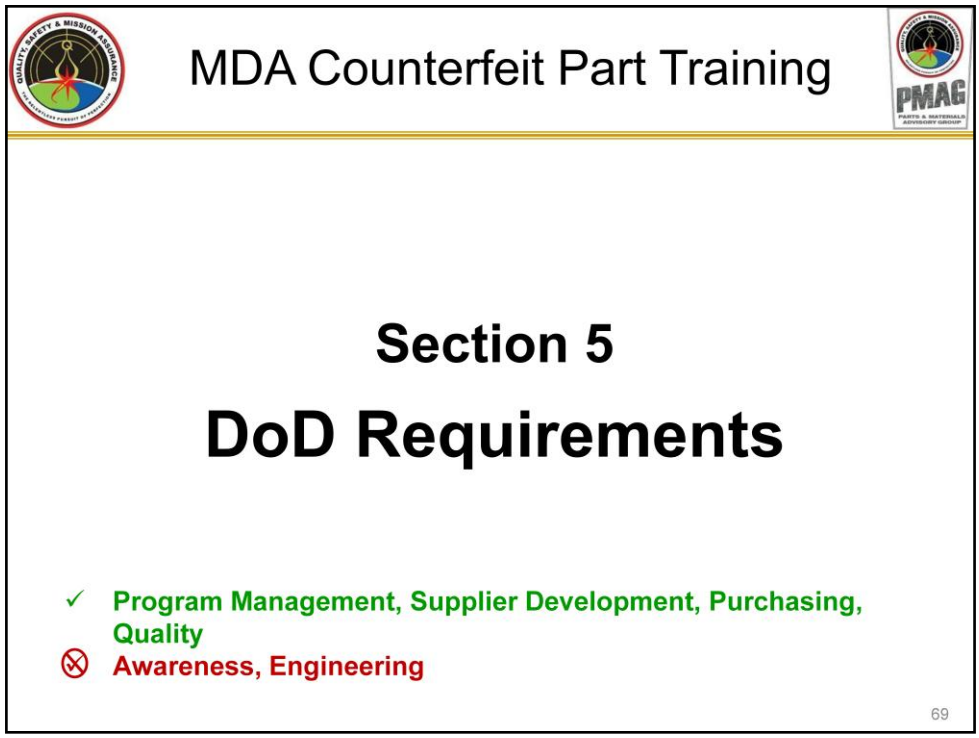
Test your knowledge of this section by reading each of the three statements. What is your answer for each one? Go to the next slide to see how you did.



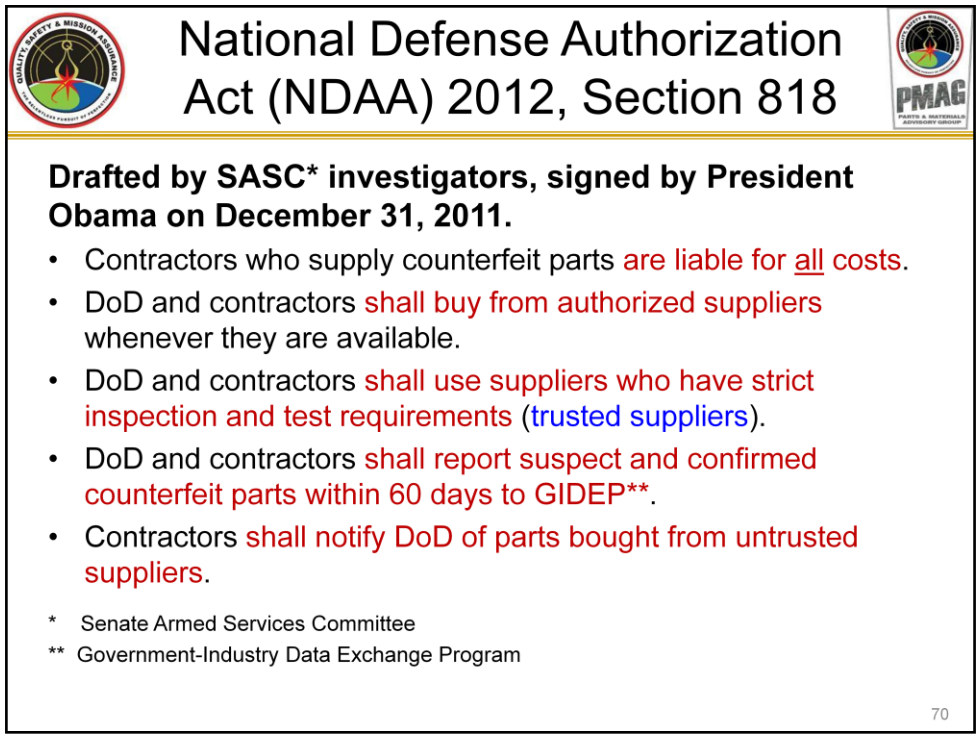
The first answer is 'true'. Probably all of MDA's detected parts would've been found immediately, if the organization had solid inspection and test methods in place at Receiving.

The second answer is 'false'. Most of MDA's detected counterfeit parts had low failure rates. In several cases there were no failures. This does not mean the parts can be counted on to perform reliably.

The third answer is 'true'. Four of the ten detected part numbers were still in production when the parts were bought. Those parts should have been bought from authorized suppliers, in compliance with Rule #1.

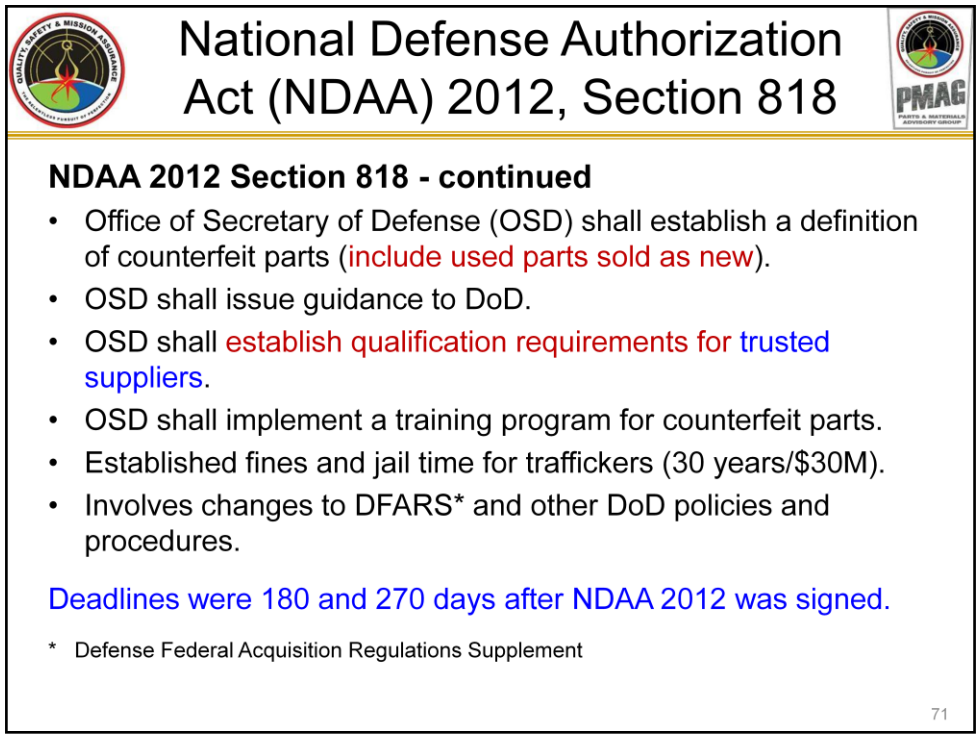


This section touches on the various requirements flowed to or from the Department of Defense to date. As you will see, OSD and DoD's reaction to counterfeit parts is still in development. 2013 will see the release of additional policies or procedures to combat counterfeit electronic parts.



Because of the November 2011 Senate Armed Services Committee hearing, Section 818 was added to the 2012 National Defense Authorization Act, or NDAA, to force DoD into implementing robust anti-counterfeit procedures. This slide and the next one detail the more important requirements from Section 818:

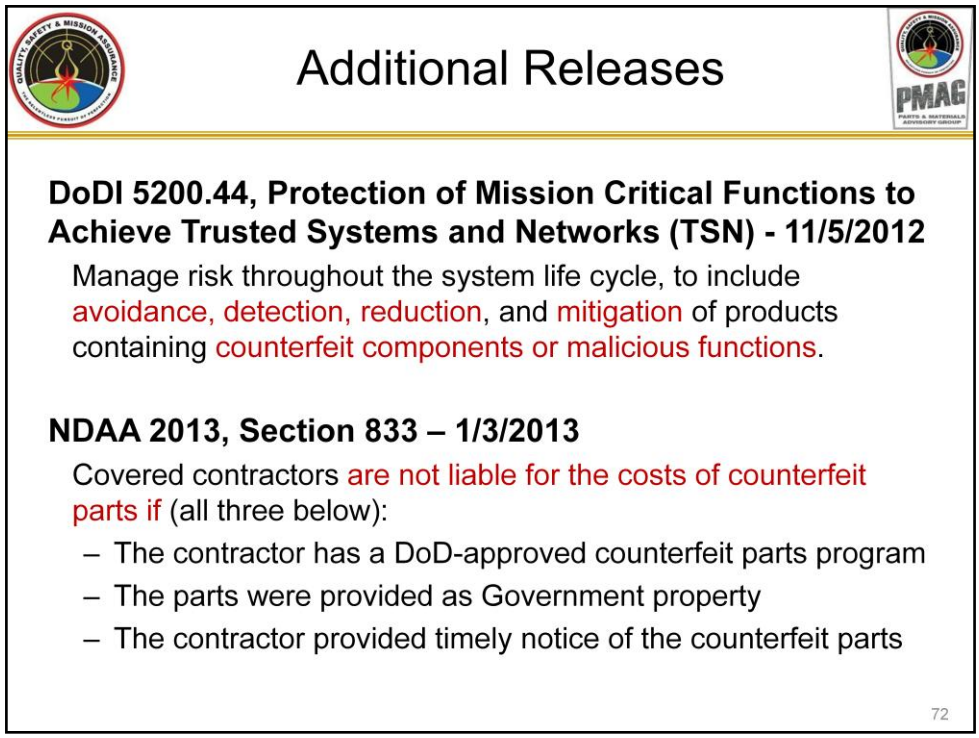
1. Covered contractors are liable for all costs of counterfeit parts, including system repair and rework. This requirement was loosened somewhat in 2013.
2. DoD and contractors are directed to buy only from authorized suppliers or the OCM.
3. DoD and contractors are directed to use trusted suppliers when parts are no longer available in production, and those trusted suppliers shall be flowed strict inspection and test requirements.
4. DoD and contractors are directed to report all suspect or confirmed counterfeit parts to the Government-Industry Data Exchange Program, or GIDEP, within 60 days of discovery.
5. Contractors are directed to notify the Government if parts cannot be bought from authorized or trusted suppliers.



Additional major requirements of NDAA 2012 Section 818 are:

1. The Office of the Secretary of Defense, or OSD, is directed to establish a definition of counterfeit parts. The definition shall include used parts sold as new.
2. OSD shall also provide guidance to DoD on counterfeit electronic parts avoidance.
3. OSD shall establish qualification requirements for trusted suppliers.
4. OSD shall develop a training program for DoD.
5. Fines and jail times up to 30 years or $30 million for repeat offenders who knowingly supply counterfeit parts to DoD.
6. OSD was directed to revise the Defense Federal Acquisition Regulations Supplement, or DFARS (pronounced DEE-farz), to address the prevention and detection of counterfeit electronic parts. The revision is still in development.

The deadlines for implementation on the program were 180 days and 270 days after signoff of the document, or June and September of 2012. While some of the changes have been implemented, such as the counterfeit parts definition, and DoD guidance, there are many requirements that are not as yet implemented.



In November of 2012, DoD released the 5200.44 instruction, titled “Protection of Mission Critical Functions to Achieve Trusted Systems and Networks”, also known as TSN. This instruction directed the use of the Program Protection Plan, and Information Assurance, to manage risk throughout a system’s life cycle. There is a requirement to detect, reduce, and mitigate the risk of counterfeit or malicious parts or functions.

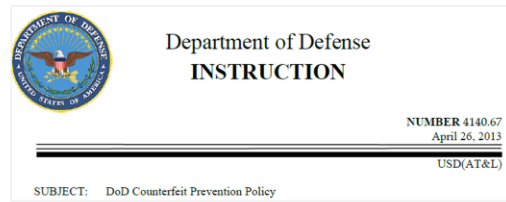
There was also modification to the requirements of NDAA 2012, Section 818. These allowances were signed into law on January 3, 2013, as Section 833 of the National Defense Authorization Act for 2013. Section 833 allows for covered contractors to be relieved of the liability costs for counterfeit electronic parts if all three of the following items are true:

1. The contractor has a counterfeit parts program that has been reviewed and approved by DoD.
2. The parts were provided as Government property.
3. The contractor has complied with the NDAA 2012 Section 818 requirements for prompt reporting of counterfeit parts.

DoD Instruction 4140.67 (DoDI 4140.67)

DoD Instruction 4140.67, "DoD Counterfeit Prevention Policy", was released on April 26, 2013.

- Supersedes and cancels the 'Kendall Memorandum'.
- Policy includes anti-counterfeit measures for avoidance, detection, mitigation, investigation, reporting, and restitution.
- Applies to all materiel, no special policy or guidance for electronic parts.



Department of Defense
INSTRUCTION

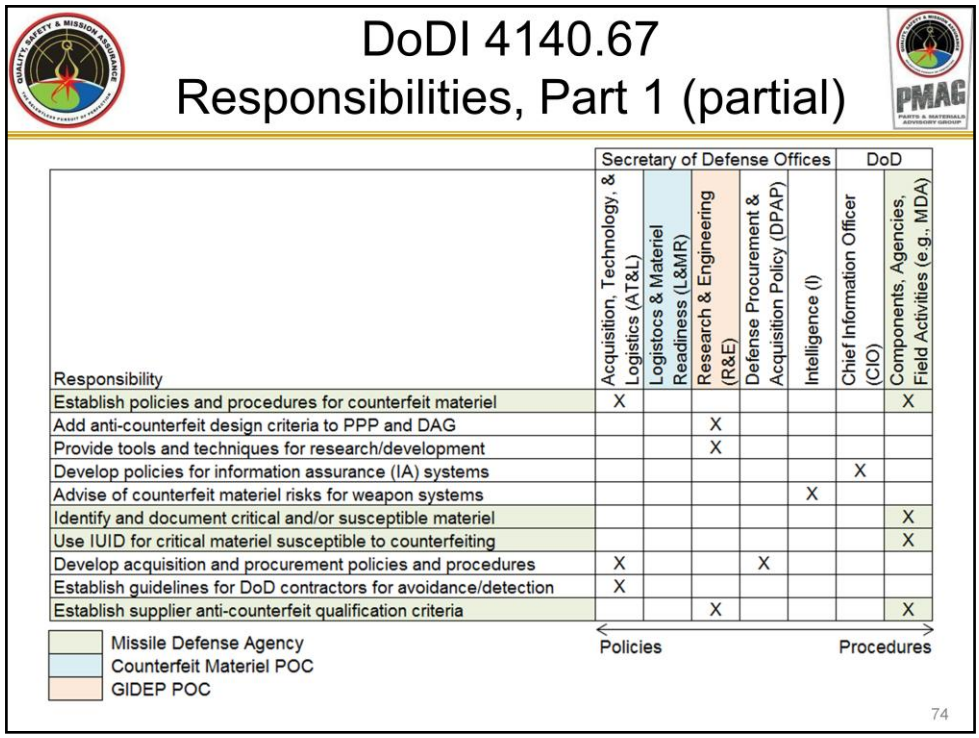
NUMBER 4140.67
April 26, 2013

USD(AT&L)

SUBJECT: DoD Counterfeit Prevention Policy

73

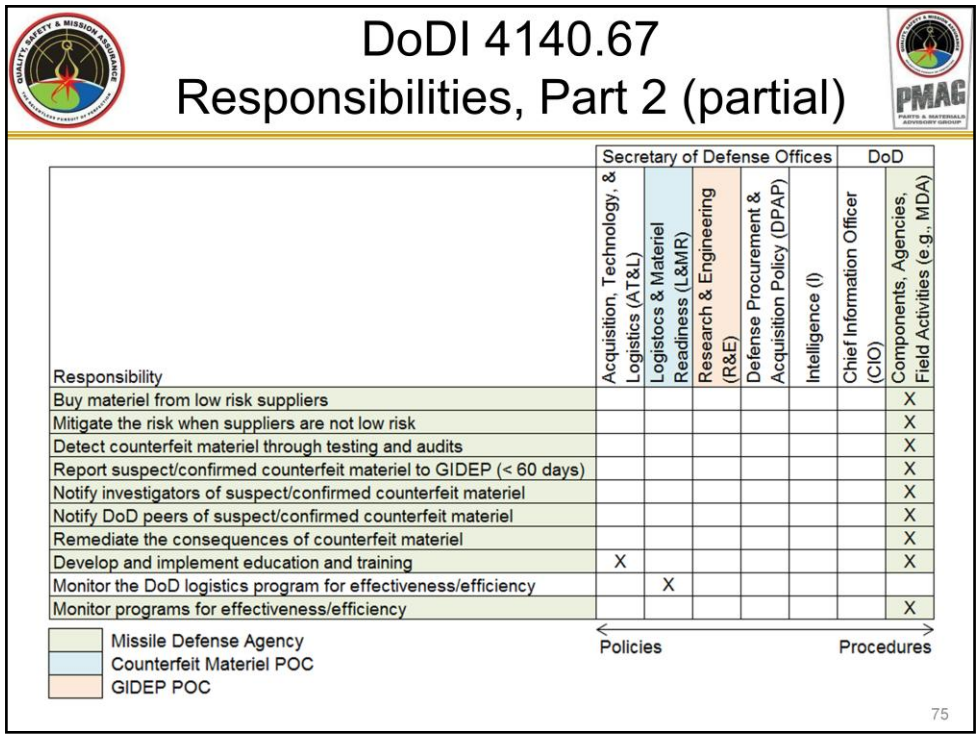
In April 2013, OSD released DoD Instruction 4140.67, titled "DoD Counterfeit Prevention Policy". This instruction superseded and cancelled the interim Kendall Memorandum from 2012. The policy establishes anti-counterfeit measures for avoidance, detection, mitigation, investigation, reporting, and restitution. Unlike the prior memorandum which requires actions in some cases specific to electronic parts, DoDI 4140.67 applies to all materiel. The guidance and policy do not specifically address electronic parts.



This slide and the next one list the major requirements of DoDI 4140.67, with the responsible DoD party listed for each requirement. The green highlighted items fall under the responsibility of Component and Agency Heads, including the Missile Defense Agency. While those items in the left columns tend to be policies, the right columns are generally expected to develop procedures to implement those policies.

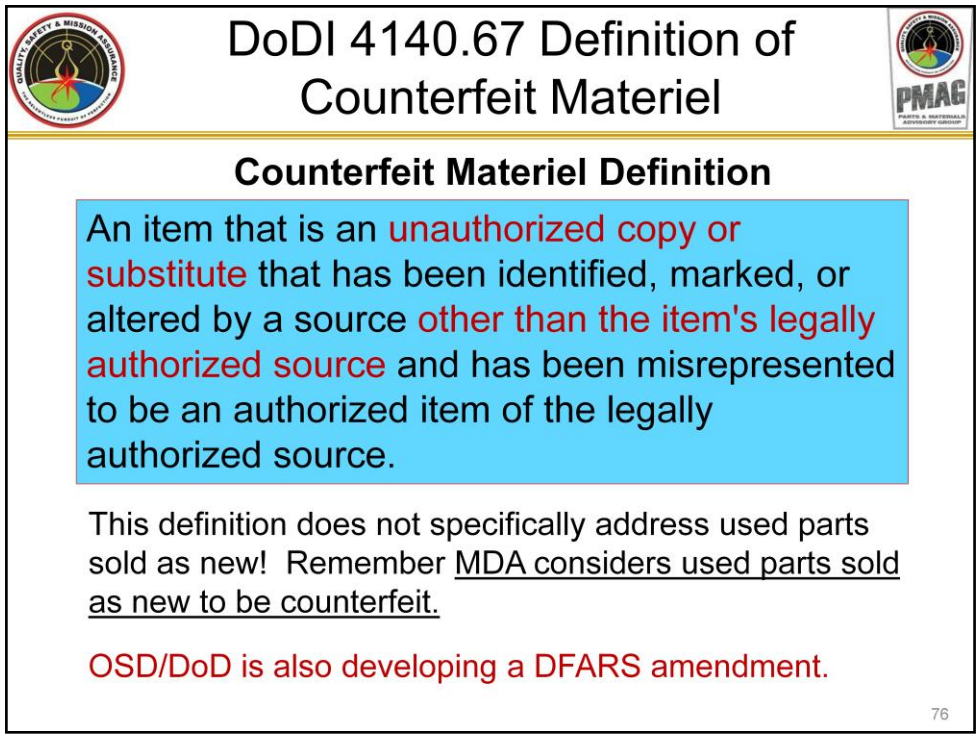
In this slide, MDA is tasked to develop anti-counterfeit procedures, like the PMAP. We are also required to identify and document critical materiel, as well as materiel that is more susceptible to counterfeiting. MDA is also directed to use Item Unique Identification, or IUID, per DoD Instruction 8320.04, for critical materiel that is susceptible to counterfeiting.

DoD Components are directed to establish supplier qualification criteria for managing the counterfeit materiel risk.



Procedures must also force the purchase of materiel from low-risk suppliers, and have mitigation processes for high-risk supplier purchases. Additionally, there are requirements to detect parts through testing and audits, report suspect and confirmed counterfeit parts to GIDEP, and notify investigators as well as DoD peers. DoD Components must also remediate the occurrences of counterfeit materiel.

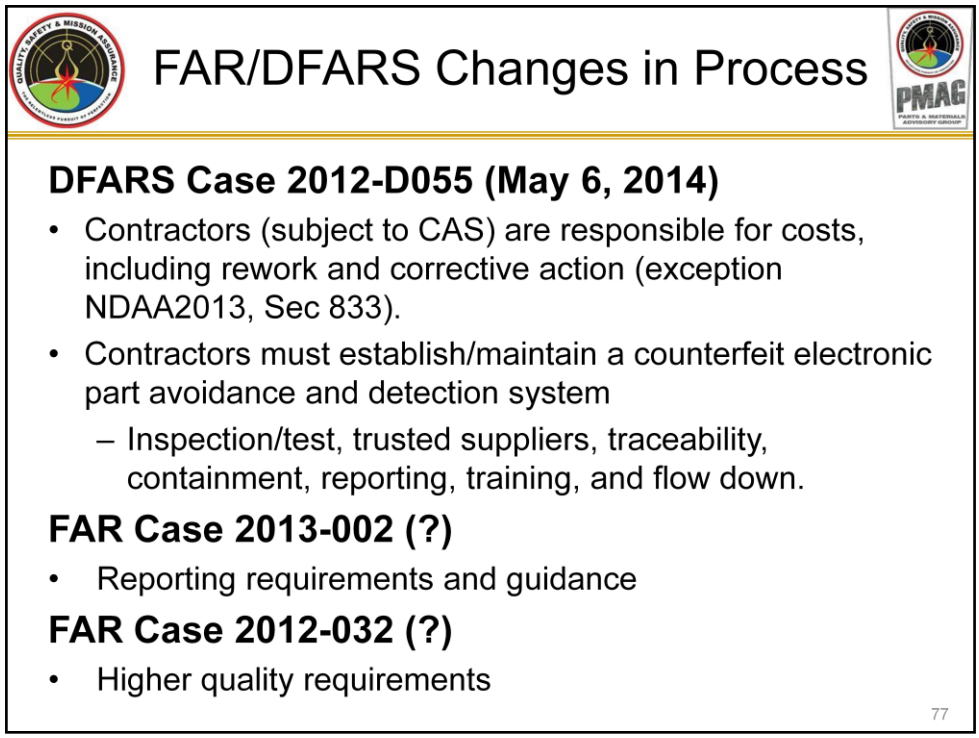
Components are directed to implement training and education programs, like this course, to their workforce. And finally, DoD Components are to develop metrics that will enable the effectiveness and efficiency of the procedures to be monitored.



Shown here is the DoD definition of counterfeit materiel as stated in the April 2013 DoD Instruction. The term 'materiel' refers to electronic parts, mechanical parts, assemblies, material, etc.

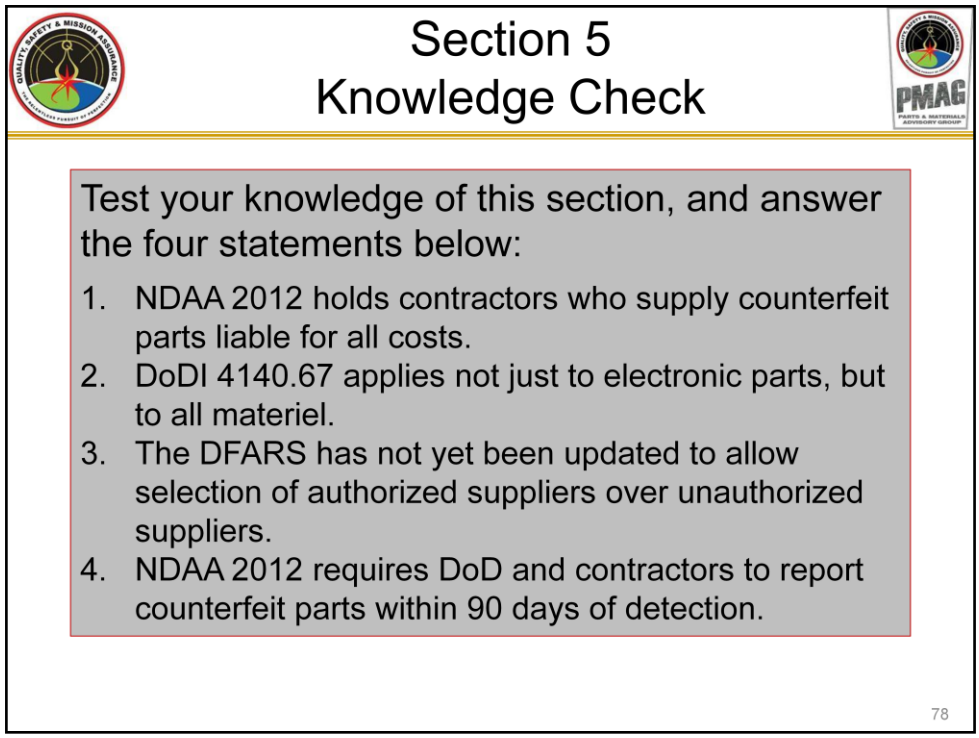
Unfortunately, DoDI 4140.67 does not specifically address used electronic parts sold as new components. Therefore, we remind you of Section 1, and that MDA does consider new parts sold as new to be counterfeit, even if they have not been remarked or recoated.

In addition to the documents discussed previously, there is an effort underway to modify the Defense Federal Acquisition Regulations Supplement, or DFARS, to allow DoD Components greater flexibility to select authorized suppliers for electronic parts.

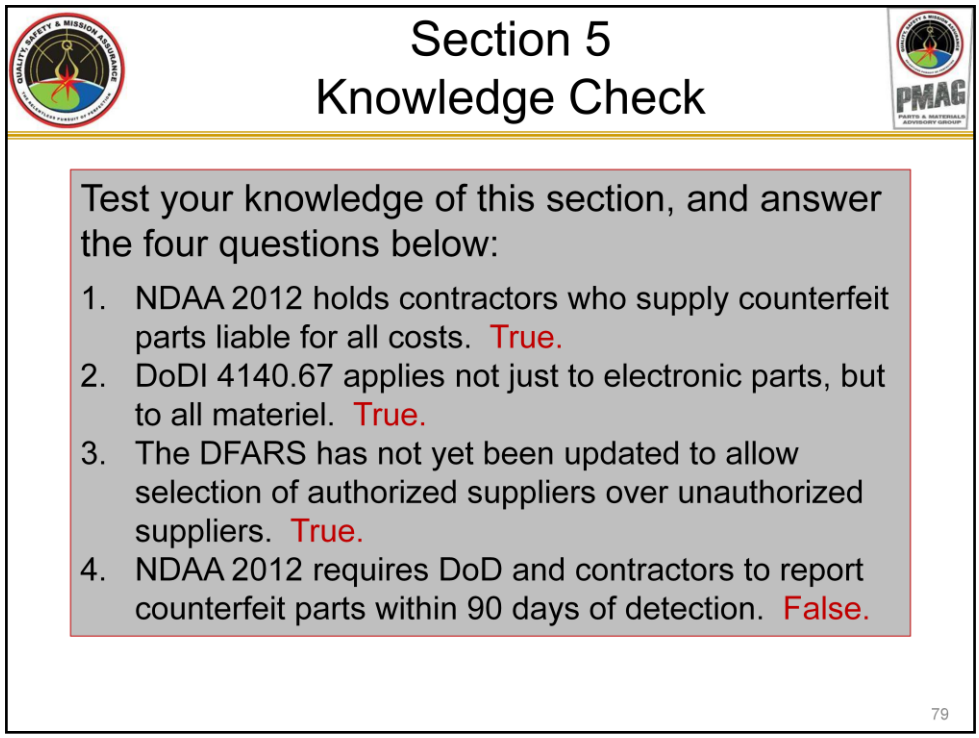


Three more proposed changes to DoD acquisition requirements are planned. The first case, DFARS Case 2012-D055, is in its second revision, and might be released later this year. While establishing contractor liability for costs, and requirements for the contractors' counterfeit electronic part avoidance and detection system, the current draft does not require purchases from authorized suppliers as a first choice, nor is it very specific on other requirements.

The next two amendments in process are to change changes to the Federal Acquisition Regulations, or FAR. The changes are reportedly to add reporting and quality requirements, although neither of these draft has been released yet.



Test your knowledge of this section by reading each of the four true/false statements. What is your answer for each one? Go to the next slide to see how you did.

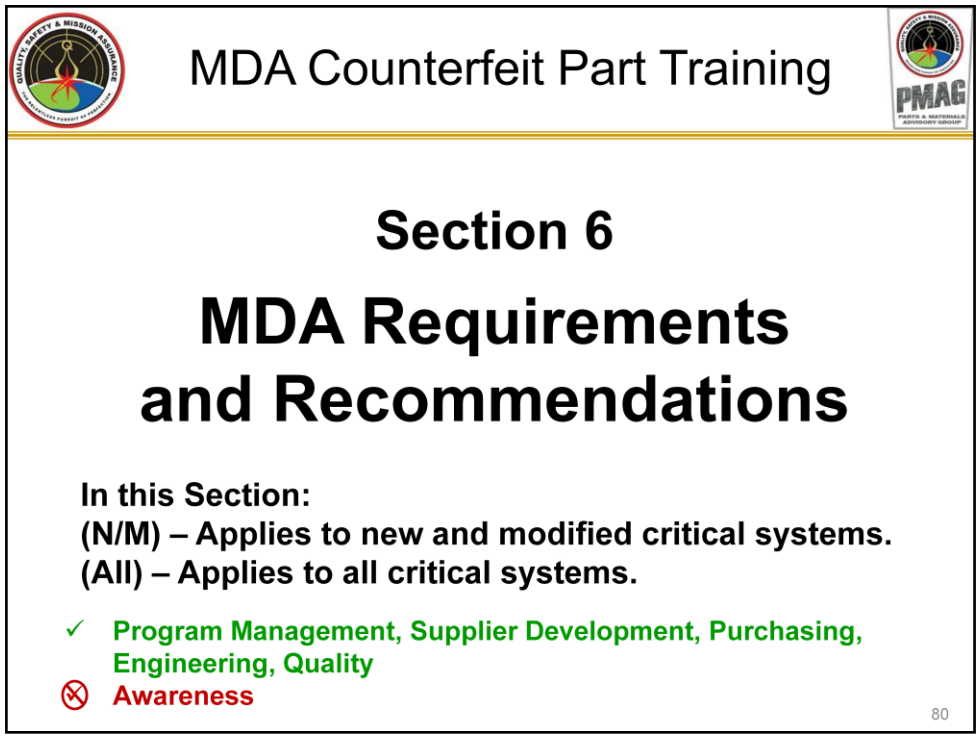


The first statement is true. According to Section 818, contractors who supply counterfeit parts are liable for all costs, including repair and rework.

The second statement is true. DoD Instruction 4140.67 establishes policy for all materiel. However, once critical and susceptible materiel is identified, the list of affected materiel will be significantly reduced.

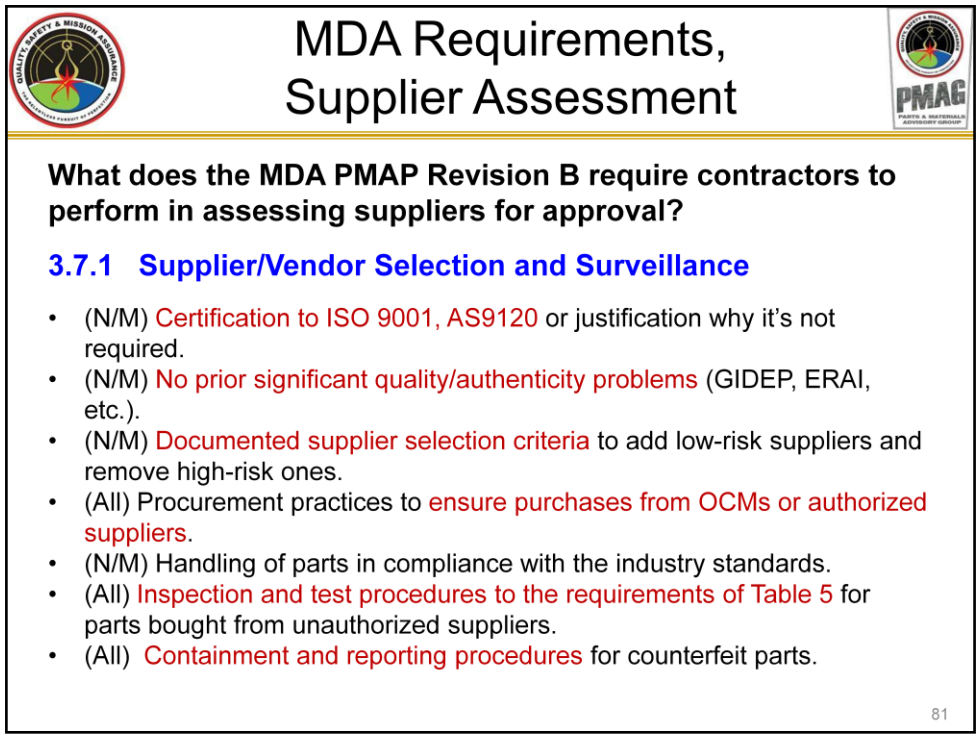
The third statement is true. The Defense Federal Acquisition Regulations Supplements, or DFARS, has not yet been revised to allow purchasers more freedom to buy from authorized suppliers.

The fourth statement is false. DoD and contractors are required to report counterfeit parts to GIDEP, but the deadline is 60 days after detection, not 90 days.



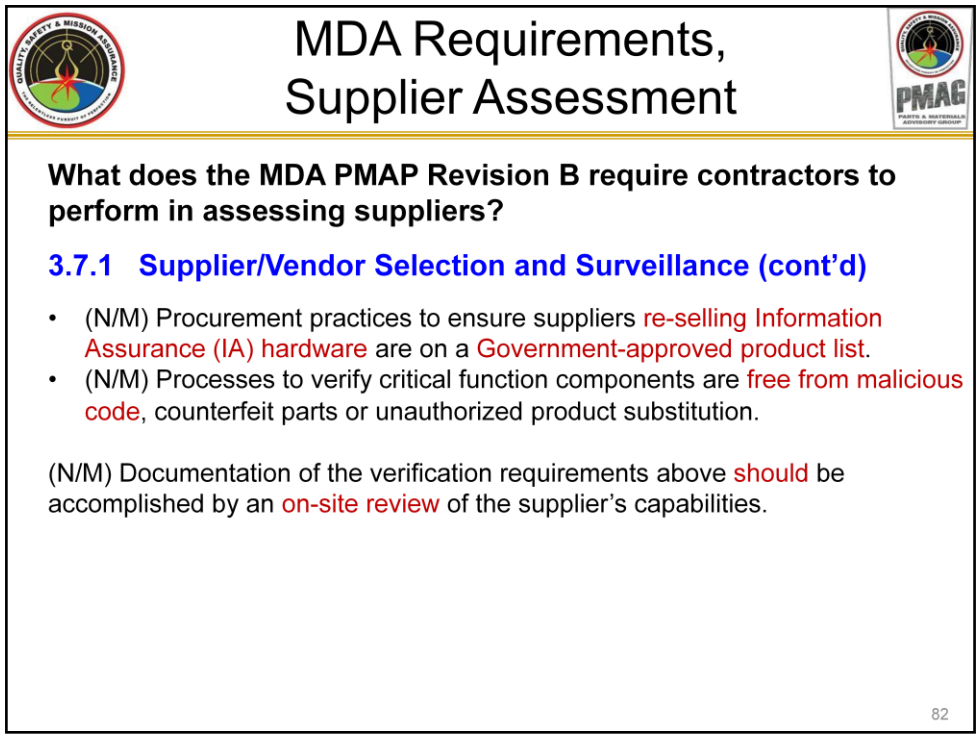
This section gives a detailed overview of MDA's current requirements for avoiding, detecting, containing, reporting, disposing, and otherwise mitigating the risk of counterfeit parts.

In this section you will see '(N/M)' and '(All)' designations next to the requirements. This is to indicate whether that requirement applies only to new and modified critical systems via the PMAP only, or if it applies to all critical systems via both PMAP and Policy Memo #50.



With respect to selection of approved suppliers, there are several requirements, as indicated on the next two slides. Remember, approved suppliers have been assessed by the contractor and found acceptable to provide electronic parts. The requirements include:

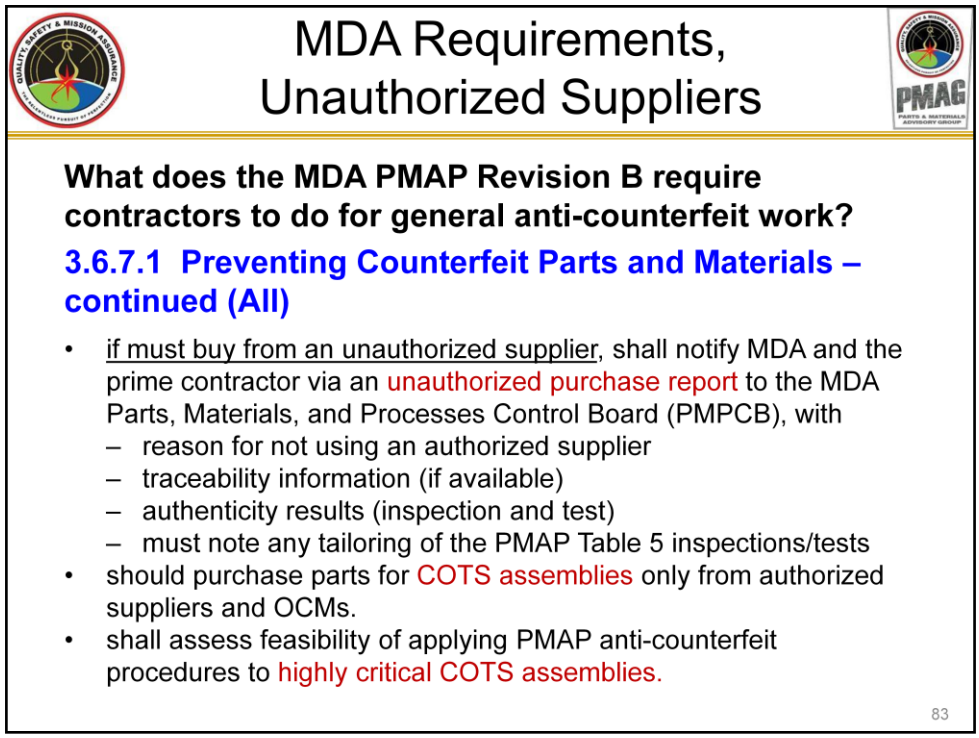
1. Suppliers shall be certified to ISO 9001, AS 9120, or an equivalent quality standard, or justify why not.
2. Suppliers shall have no significant quality or authenticity problems, as found in the GIDEP or ERAI databases.
3. Suppliers shall have documented criteria for adding and removing suppliers from their approved supplier listing.
4. Suppliers shall always buy parts from authorized suppliers or OCMs as a first priority.
5. Handling of parts shall comply with electrostatic discharge and moisture sensitivity industry standards.
6. Suppliers shall perform specific inspections and test for parts bought from unauthorized suppliers.
7. Suppliers shall contain and report counterfeit parts.



Additional supplier assessment requirements include:

1. Authorized Information Assurance, or IA, hardware suppliers shall be on a Government-approved list.
2. Processes shall attempt to ensure critical components are free from malicious code, counterfeit parts, or unauthorized part substitution.

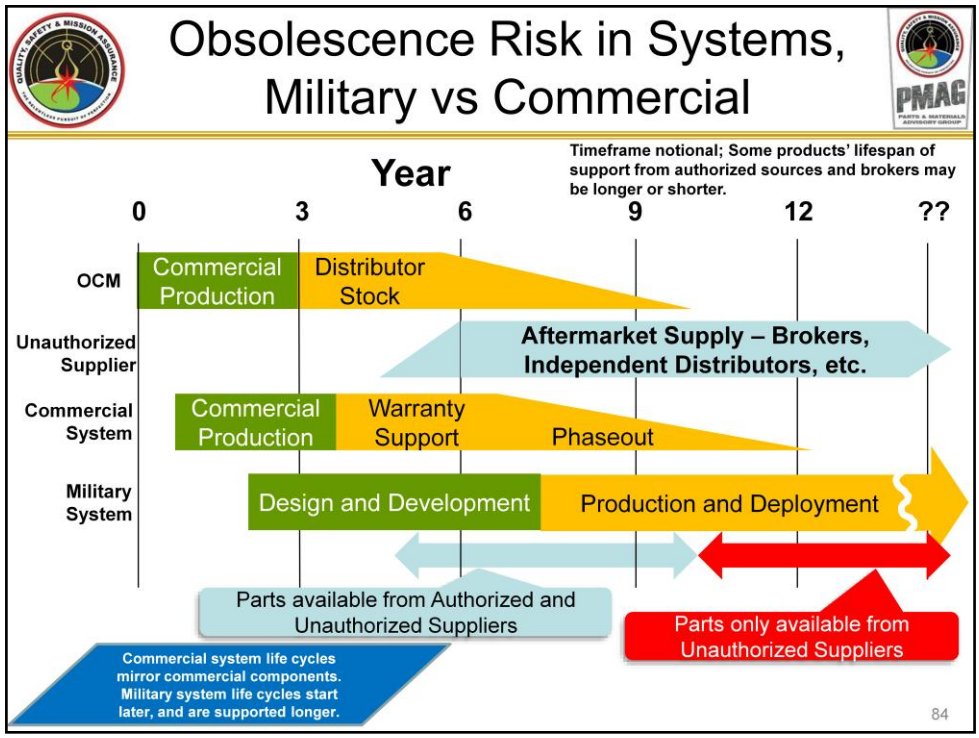
MDA encourages the approval of unauthorized suppliers via on-site assessments.



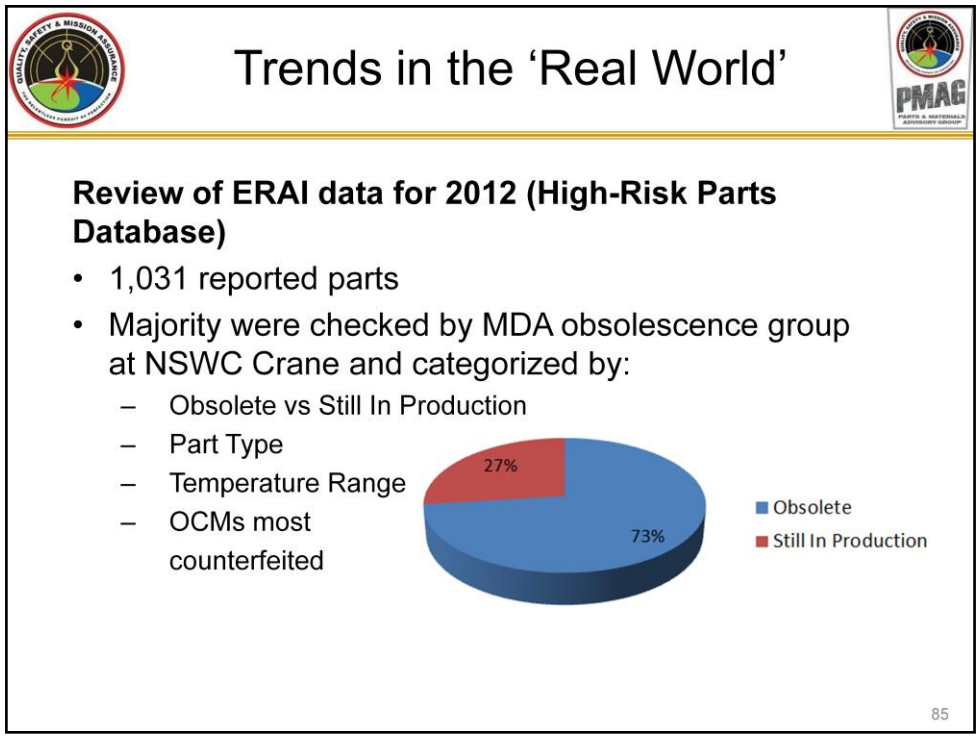
MDA also requires contractors that must buy parts from unauthorized suppliers to document this request to MDA and the prime contractor through an unauthorized purchase report. The report must:

1. Justify the reason for buying from an unauthorized supplier.
2. Provide traceability information, if available.
3. Provide the inspection and test plan and results.
4. Identify any shortened or tailored inspections or tests noncompliant to PMAP Table 5.

In addition, MDA contractors are required to assess the feasibility of applying the anti-counterfeit processes from the PMAP to critical Commercial-Off-The-Shelf, or COTS (pronounced ‘cots’) product, while limiting purchases of COTS products to authorized suppliers or OCMs.

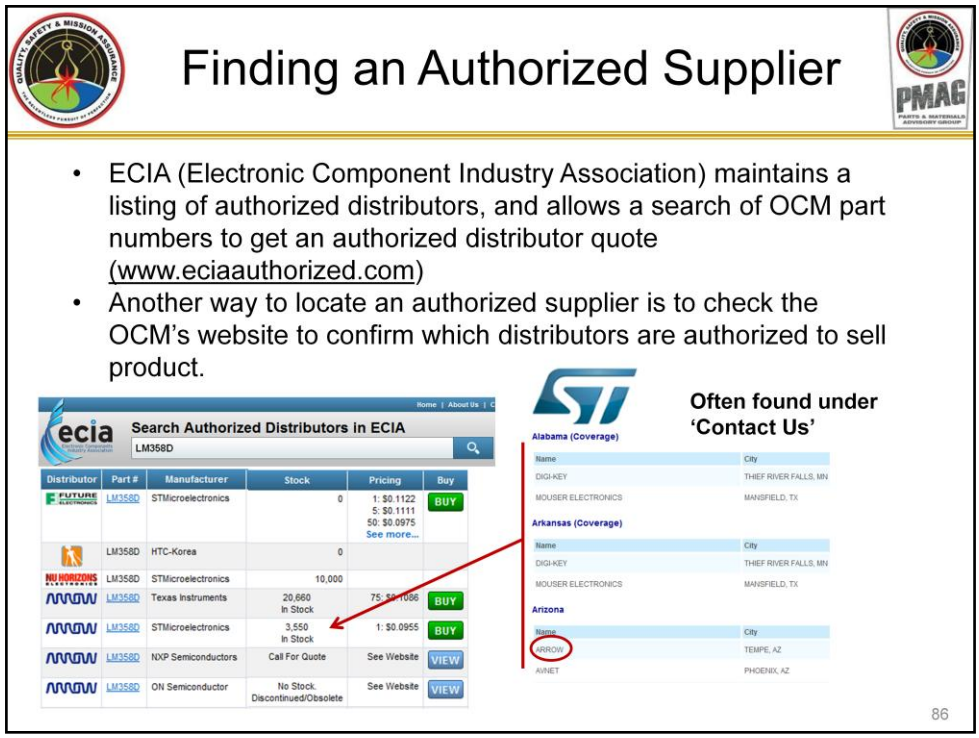


As the timeline above indicates, OCM parts like integrated circuits are usually in production several years before being designed into a military system. In addition, most military systems have life cycles much longer than their commercial counterparts. While commercial systems are often discontinued or redesigned in less than ten years, military systems may need to be supported virtually unchanged for over twenty years. This, combined with the longer initial design stage, often results in a part being discontinued by the OCM years before the system itself is discontinued. The end result is that parts must be procured and stored as part of a lifetime buy, or unauthorized suppliers must be used to try to find authentic parts.



ERAI maintains a database of reported suspect counterfeit parts. MDA performed an analysis of over 1,000 suspect counterfeit electronic part reports in 2012. NSWC Crane maintains an obsolescence database of thousands of parts, that allows characterization of the data by part type, obsolescence, temperature range, and component manufacturer, or OCM.

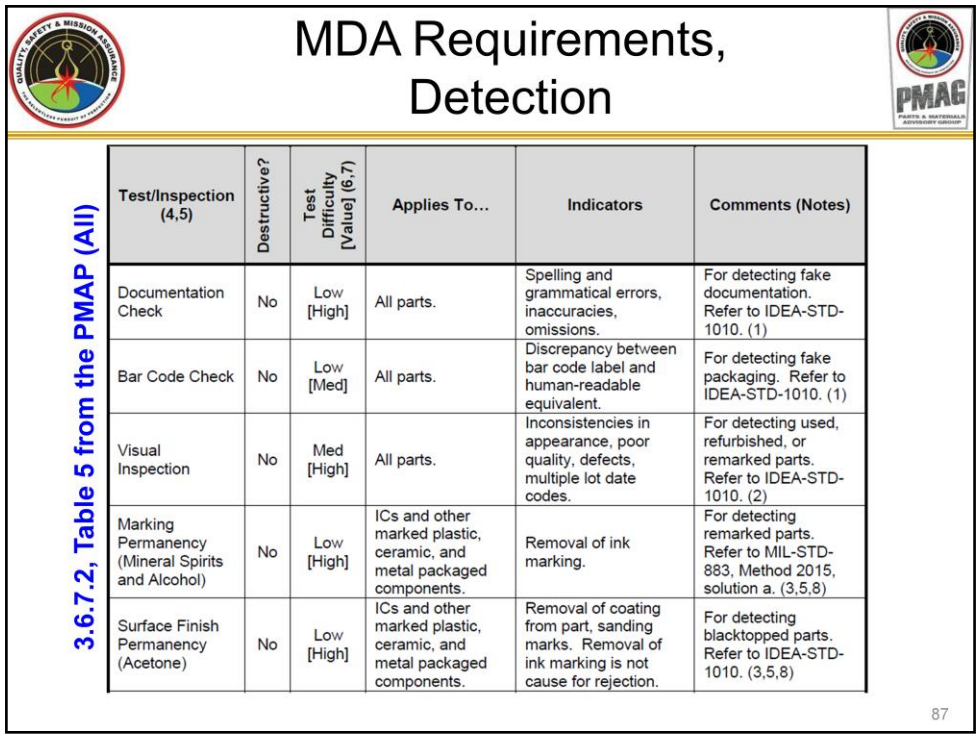
As indicated in the pie chart, almost three fourths of the reported parts were obsolete at the time of detection. This means that over 250 of the ERAI-reported suspect counterfeit parts from 2012 would not have been bought if the company had only followed Rule #1, and bought the parts from authorized suppliers.



The two best ways to find out whether a distributor is authorized to sell a particular OCM's product are to:

1. Use the website www.eciaauthorized.com to find authorized suppliers and available parts for a particular part number. See the left graphic example of a search for the LM358D, which found ST Microelectronics parts available from authorized distributors Nu Horizons and Arrow, for about 10 cents each.
2. Call the OCM or check the 'Contact Us' tab on the website to determine which distributors are authorized. See the right graphic example which shows Digi-Key, Mouser, Arrow, and Avnet are among the authorized distributors for ST Microelectronics parts.

Don't ever rely on the distributor's response about whether it is authorized for an OCM.



MDA Requirements, Detection

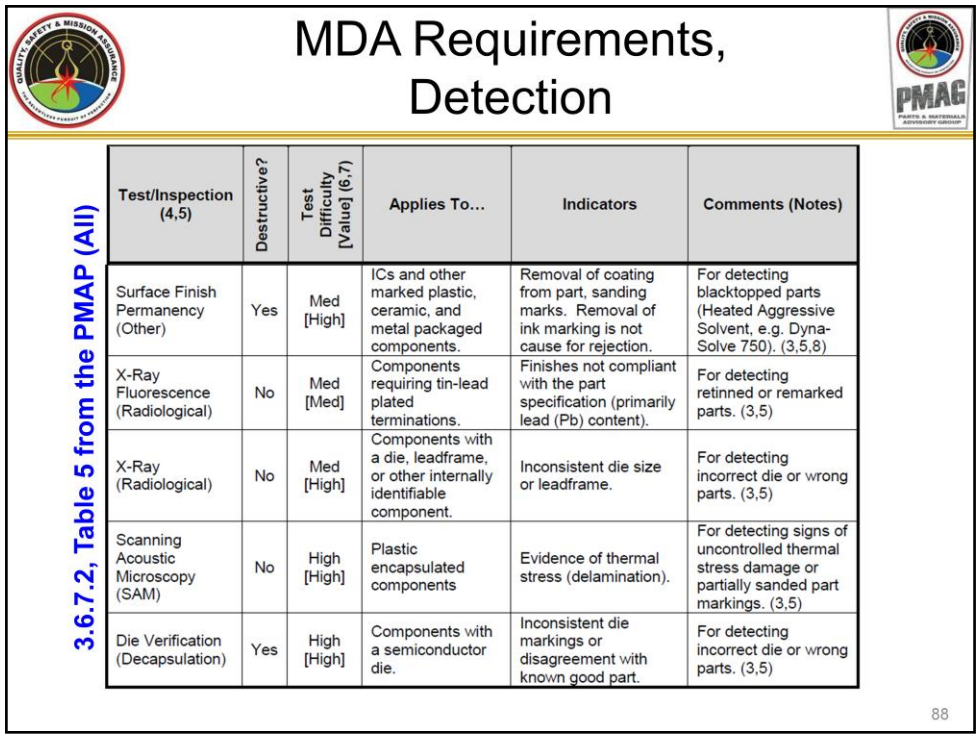
3.6.7.2, Table 5 from the PMAP (All)

Test/Inspection (4,5)	Destructive?	Test Difficulty [Value] (6,7)	Applies To…	Indicators	Comments (Notes)
Documentation Check	No	Low [High]	All parts.	Spelling and grammatical errors, inaccuracies, omissions.	For detecting fake documentation. Refer to IDEA-STD-1010. (1)
Bar Code Check	No	Low [Med]	All parts.	Discrepancy between bar code label and human-readable equivalent.	For detecting fake packaging. Refer to IDEA-STD-1010. (1)
Visual Inspection	No	Med [High]	All parts.	Inconsistencies in appearance, poor quality, defects, multiple lot date codes.	For detecting used, refurbished, or remarked parts. Refer to IDEA-STD-1010. (2)
Marking Permanency (Mineral Spirits and Alcohol)	No	Low [High]	ICs and other marked plastic, ceramic, and metal packaged components.	Removal of ink marking.	For detecting remarked parts. Refer to MIL-STD-883, Method 2015, solution a. (3,5,8)
Surface Finish Permanency (Acetone)	No	Low [High]	ICs and other marked plastic, ceramic, and metal packaged components.	Removal of coating from part, sanding marks. Removal of ink marking is not cause for rejection.	For detecting blacktopped parts. Refer to IDEA-STD-1010. (3,5,8)

87

MDA's PMAP Table 5 requires specific part-level inspections and tests for all parts bought from unauthorized suppliers. Those required inspections and tests are called authenticity tests, and they are listed on the next three slides. They include:

1. Documentation check, which checks for spelling, grammatical, or other errors in the part or packaging labels and paperwork.
2. Bar code check, which compares human-readable information with the corresponding machine-readable data.
3. Visual inspection to the guidelines of IDEA-STD-1010 , the latest revision.
4. Marking permanency test with mineral spirits and alcohol, to see if ink markings or false coatings are removed.
5. Surface finish permanency test with acetone, to see if false coatings are removed.



MDA Requirements, Detection

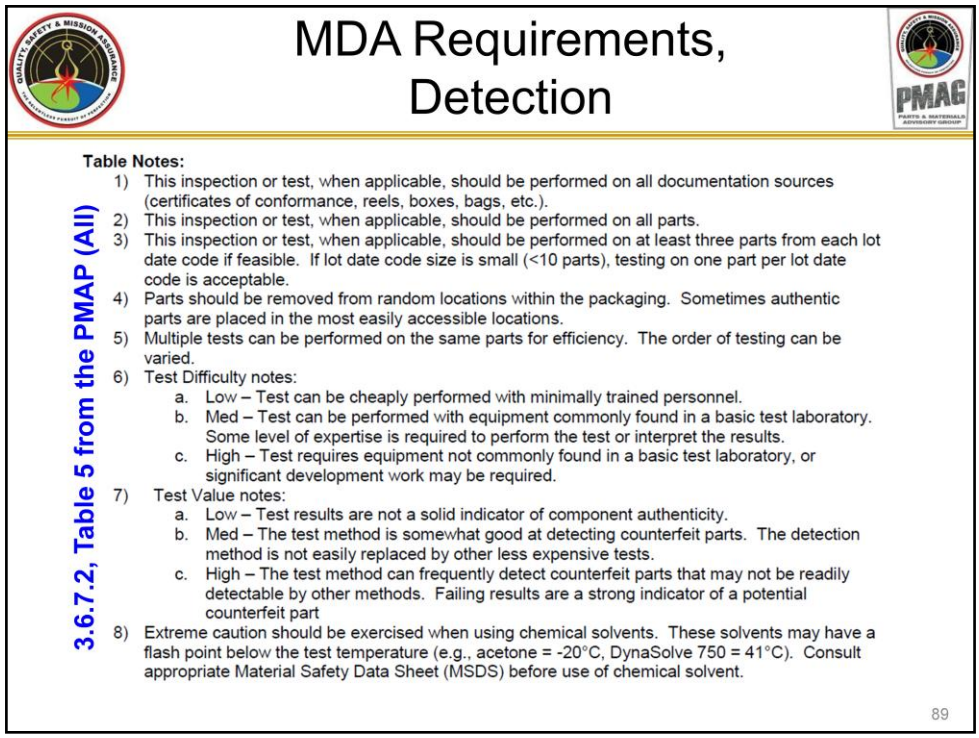
3.6.7.2, Table 5 from the PMAP (All)

Test/Inspection (4,5)	Destructive?	Test Difficulty [Value] (6,7)	Applies To…	Indicators	Comments (Notes)
Surface Finish Permanency (Other)	Yes	Med [High]	ICs and other marked plastic, ceramic, and metal packaged components.	Removal of coating from part, sanding marks. Removal of ink marking is not cause for rejection.	For detecting blacktopped parts (Heated Aggressive Solvent, e.g. Dyna-Solve 750). (3,5,8)
X-Ray Fluorescence (Radiological)	No	Med [Med]	Components requiring tin-lead plated terminations.	Finishes not compliant with the part specification (primarily lead (Pb) content).	For detecting retinned or remarked parts. (3,5)
X-Ray (Radiological)	No	Med [High]	Components with a die, leadframe, or other internally identifiable component.	Inconsistent die size or leadframe.	For detecting incorrect die or wrong parts. (3,5)
Scanning Acoustic Microscopy (SAM)	No	High [High]	Plastic encapsulated components	Evidence of thermal stress (delamination).	For detecting signs of uncontrolled thermal stress damage or partially sanded part markings. (3,5)
Die Verification (Decapsulation)	Yes	High [High]	Components with a semiconductor die.	Inconsistent die markings or disagreement with known good part.	For detecting incorrect die or wrong parts. (3,5)

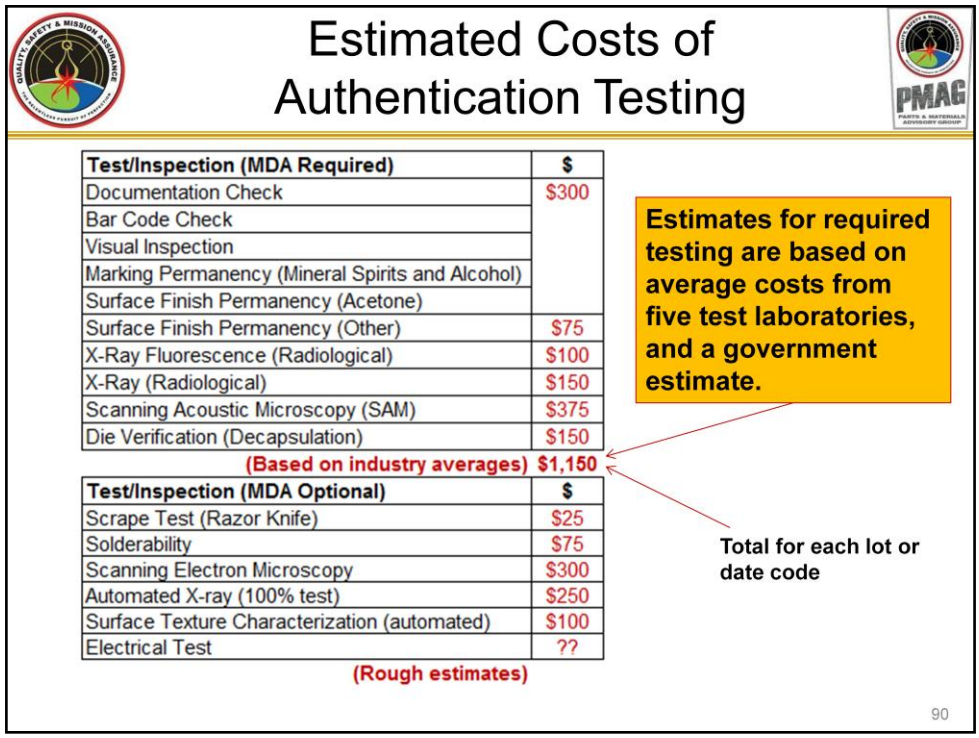
88

Continued from the previous slide, MDA's authentication testing requirements include:

6. Surface finish permanency test with aggressive solvents, to see if false coatings are removed.
7. X-ray fluorescence to determine if the lead plating is the expected composition.
8. X-ray to inspect for inconsistent die size or lead frame design.
9. Scanning acoustic microscopy, or C-SAM (pronounced 'SEE-sam) to check for internal delamination or covered laser markings.
10. Die verification to check for inconsistent die markings or the wrong OCM.



The notes list important information such as sample size, test sequence, and guidance on selecting parts. For further guidance on performing authentication testing, contact the customer or the MDA Program Office.

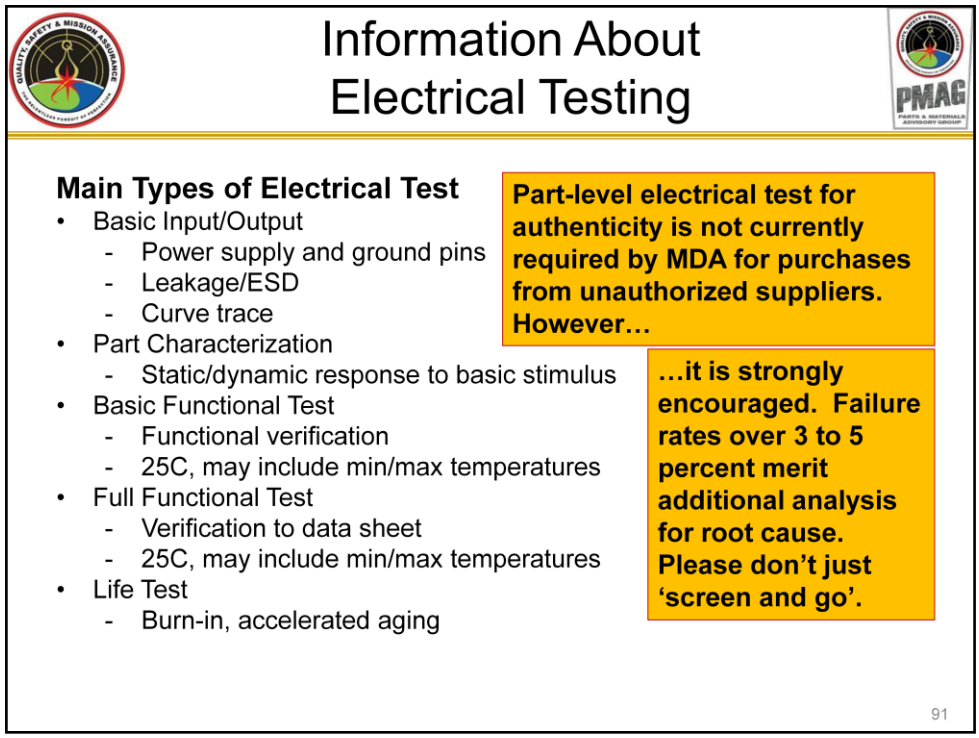


How much does it cost to validate whether a shipment of electronic parts is authentic? MDA queried five industry test laboratories, as well as a government test facility. While the estimates varied widely, the average cost of performing all of MDA's required inspections and tests should be approximately $1,150 per lot or date code. These estimates assumed the part was a medium complexity integrated circuit, although the cost did not change significantly for part complexity or lot size.

There are several other inspections and tests that can be required by an MDA contractor. These include:

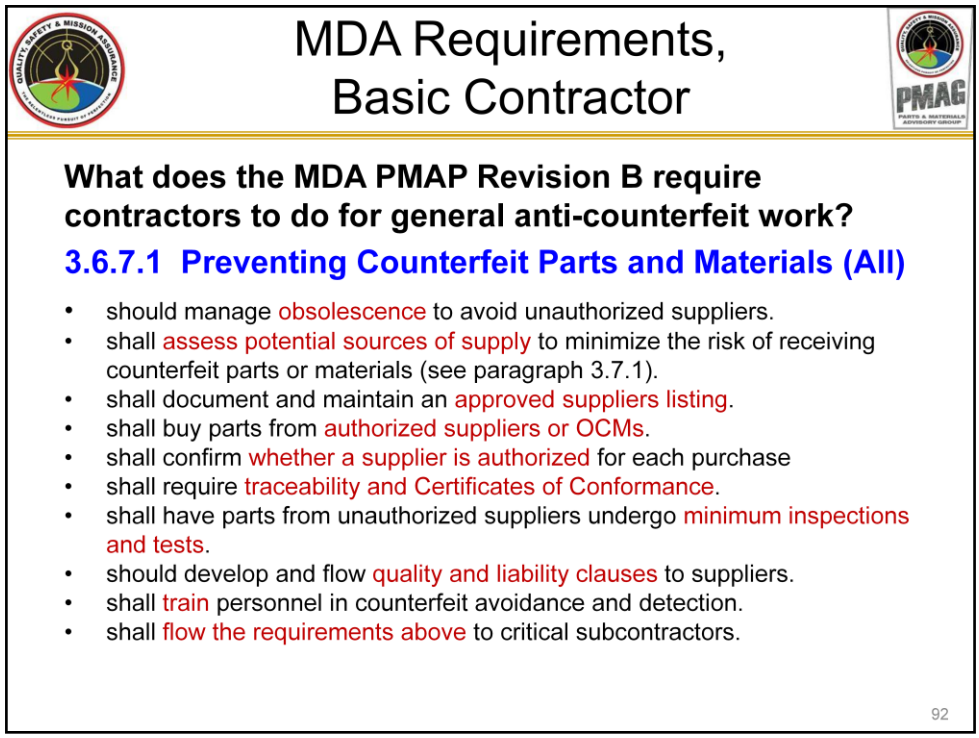
1. scraping the part's surface with a razor knife to see if coating is removed,
2. testing solderability of the part leads to see if there is contamination or oxidation,
3. magnifying the surface with a scanning electron microscope, or SEM, to inspect for signs of recoating, or of microblasting,
4. examining all the parts using an automatic-feed x-ray system to check inconsistent lead frame or die,
5. scanning the surface with equipment designed to compare surface texture differences top vs bottom, or good vs suspect, and
6. electrically testing the part to determine if it passes the selected requirements.

Electrical testing is the most difficult to estimate a cost for, as it varies widely based on the part type or complexity, the extent of testing required, and how much of the testing needs to be developed anew. This can run into the thousands of dollars very easily. The other tests are much less costly, although the estimates given here are rough at best.



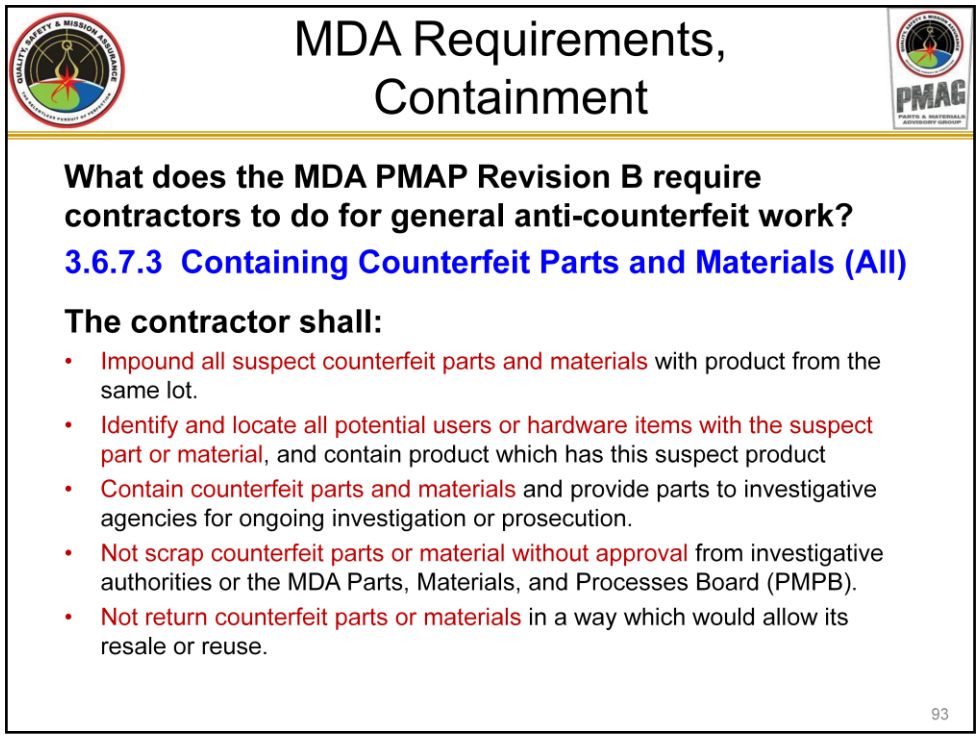
Part-level electrical test for authenticity is not currently required by MDA for parts bought from unauthorized suppliers. However, several MDA contractors do require it, with MDA's blessing. Here is a listing of several options for electrical test.

If electrical testing is performed, the failure rate should be closely monitored. Failure rates over three to five percent is cause for concern, and the contractor should consider additional analysis of the failures for root cause. Simply accepting the test as a screening process does not address the risk that the parts may have a reduced life expectancy.



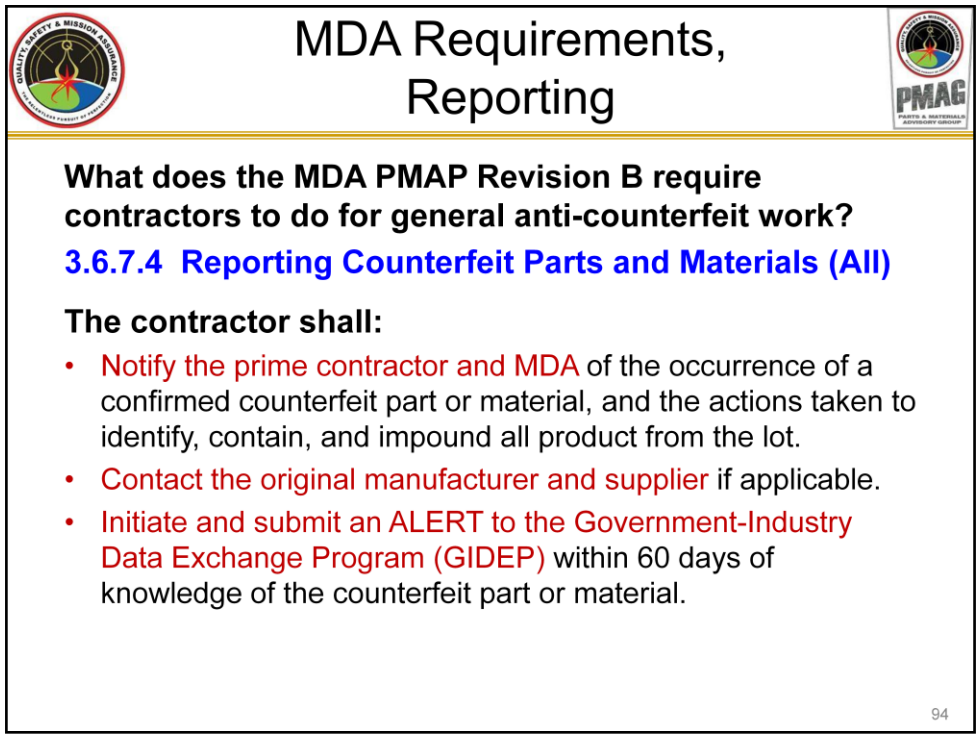
The items listed here are all requirements within MDA's PMAP. They address a couple critical processes that are contributors to the counterfeit part risk. The actual wording has been shortened, but the basic requirements are:

1. Should manage obsolescence to reduce the need to buy parts from unauthorized suppliers.
2. Shall select and confirm authorized suppliers whenever possible.
3. Shall assess unauthorized suppliers, maintain an approved suppliers listing, and require traceability and test.
4. Should develop quality and liability clauses and flow them to suppliers.
5. Shall train personnel in anti-counterfeit processes.
6. Shall flow down requirements to subcontractors.



MDA also establishes containment requirements for suspect and confirmed counterfeit parts or materials. The main requirements for performing an adequate containment are as follows:

1. Impound all suspect parts and materials.
2. Locate and contain all products with the same suspect parts or materials.
3. Contain the parts once they are determined to be counterfeit, and make them available to investigative agencies for further investigation or prosecution.
4. Retain counterfeit parts until the destruction has been approved by investigative authorities or the MDA Parts, Materials, and Processes Board, or PMPB.
5. DO NOT RETURN COUNTERFEIT PARTS.

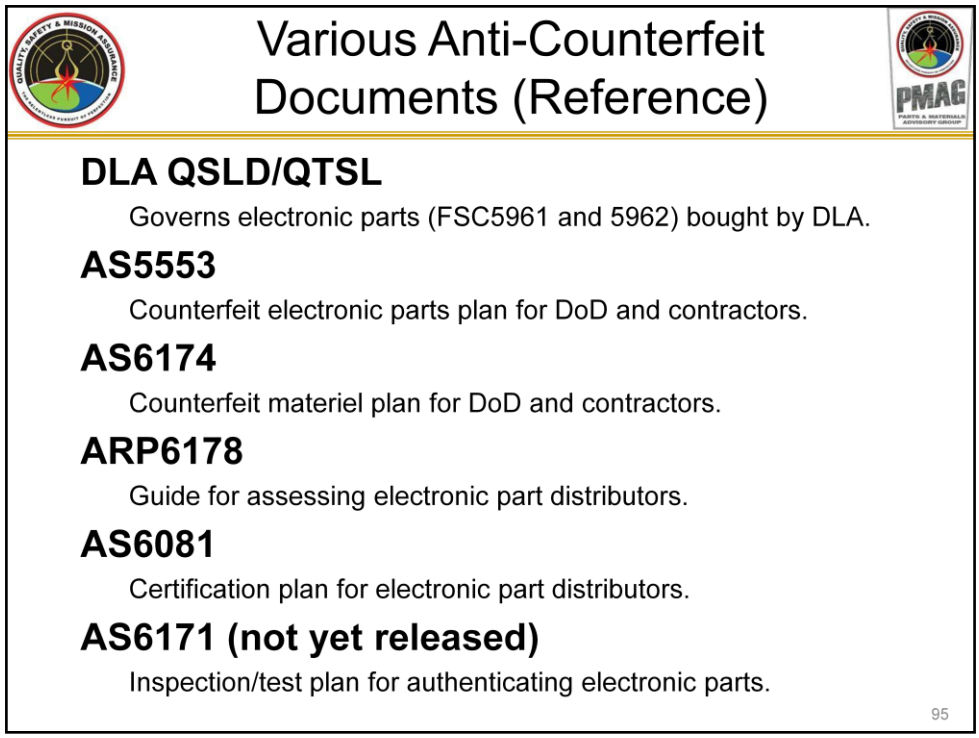


MDA specifies three straight-forward requirements to the MDA supply chain for the reporting of counterfeit parts.

First, the prime contractor and MDA must be informed of the incident. This should include a status of the containment of all affected assemblies.

Second, the contractor must contact both the supposed maker of the part – the OCM - and the supplier who provided the counterfeit parts, if that is applicable to the issue.

Third, the contractor shall submit a GIDEP alert within 60 days which documents the instance with appropriate information that may help other GIDEP members identify counterfeit parts at their own facilities.



The Defense Logistics Agency, or DLA, has established two lists, the QSLD (Qualified Suppliers List of Distributors) and QTSL (Qualified Testing Suppliers List), for combatting the risk of counterfeit electronic parts. Parts from Federal Stock Classes 5961 (semiconductors) and 5962 (integrated circuits) must be bought and tested from suppliers on these lists.

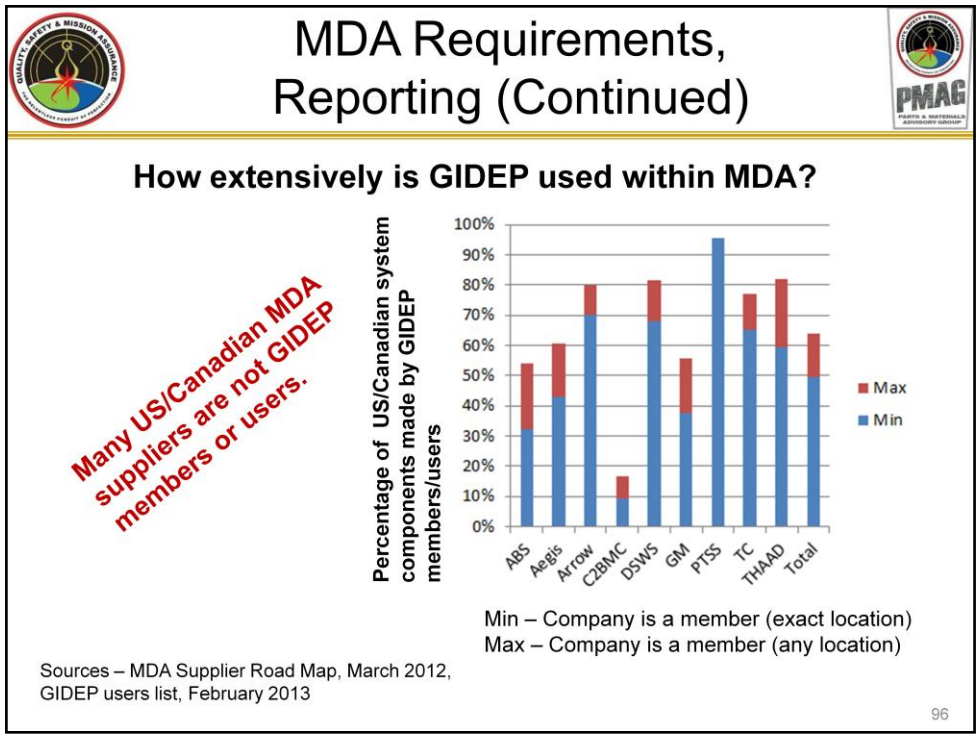
AS5553 is an anti-counterfeit document for government or aerospace organizations and contractors who use electronic parts. Organizations cannot be certified to this standard.

AS6174 is an anti-counterfeit document for government or aerospace organizations and contractors who use mechanical parts and materiel. Organizations cannot be certified to this standard.

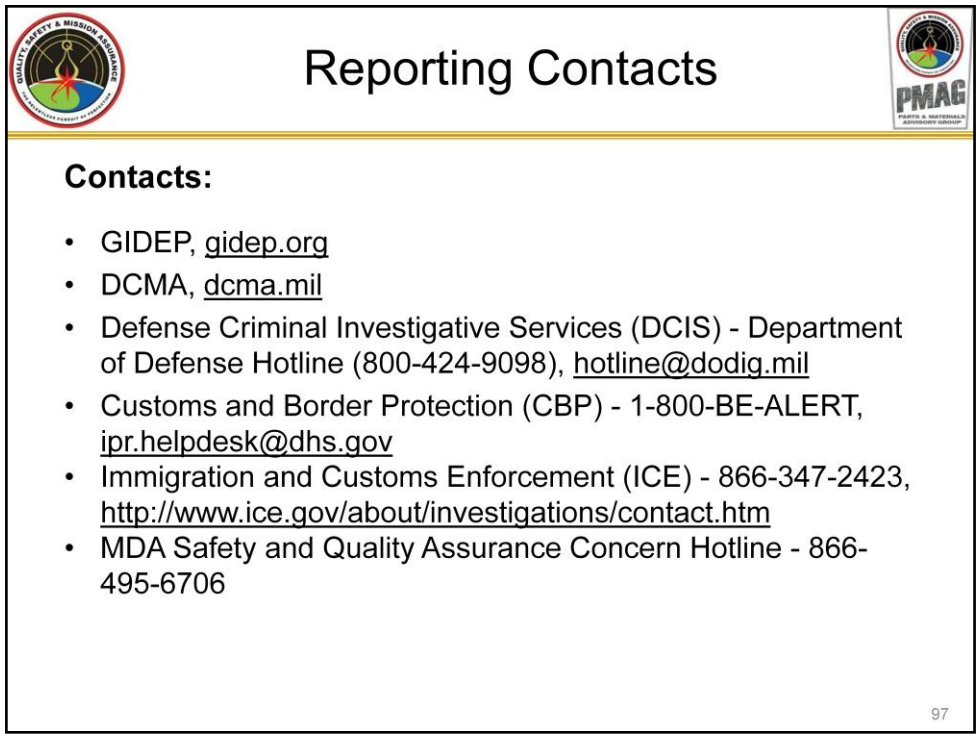
ARP6178 provides a means of numerically rating unauthorized suppliers for their risk of selling counterfeit electronic parts to government or aerospace organizations and contractors.

AS6081 is an anti-counterfeit document for distributors who sell electronic parts. Distributors can be certified to this standard.

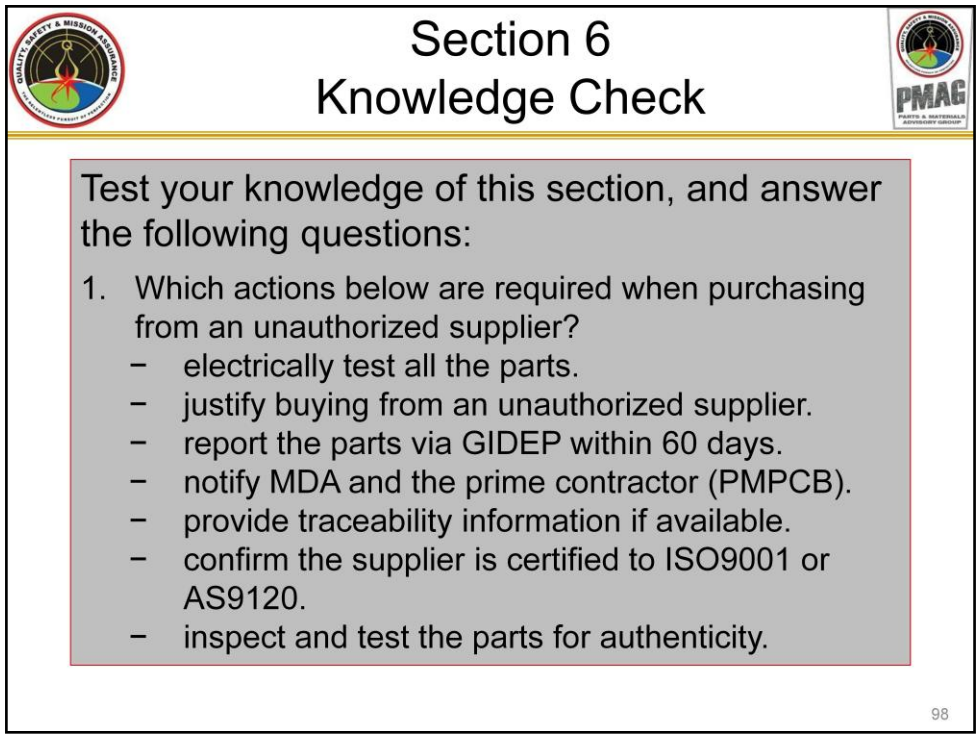
AS6171 is an inspection and test requirements document for assessing whether electronic parts are counterfeits. This document is still in development.



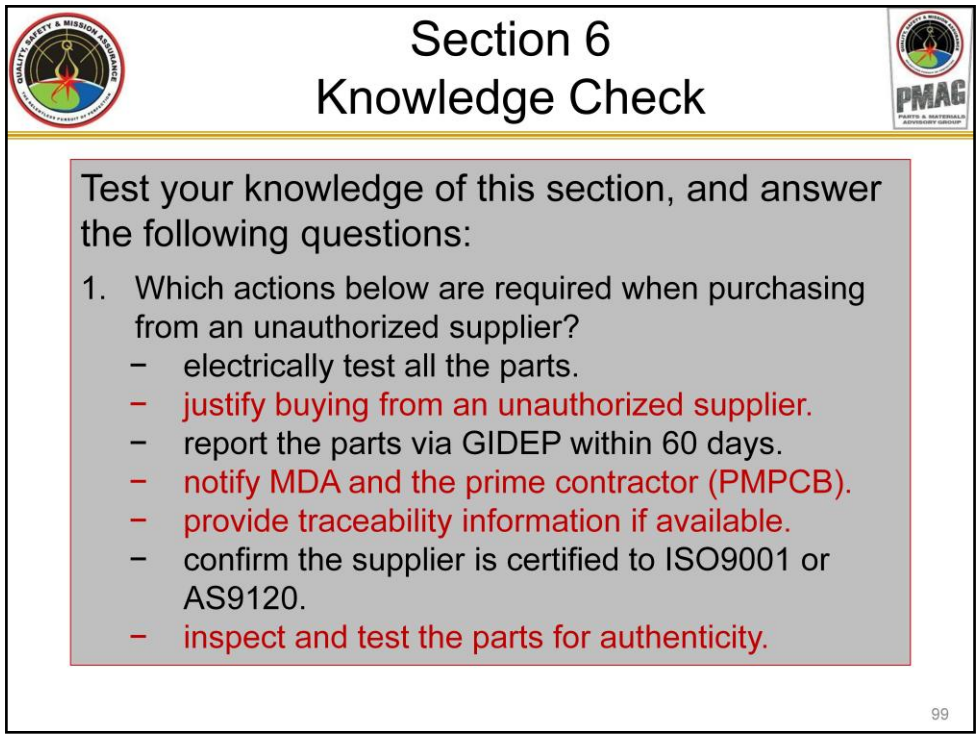
Within MDA the level of GIDEP membership is lower than it should be. This chart indicates the percentage GIDEP membership by MDA program, for Companies located in the United States or Canada. The blue line only counts if the contractor's specific location has GIDEP membership, while the red line indicates the maximum level, which counts a contractor as long as any of its locations is a member of GIDEP. The total MDA contractor membership in GIDEP appears to be 50 to 64 percent, with significant variation among programs. This should be much higher.



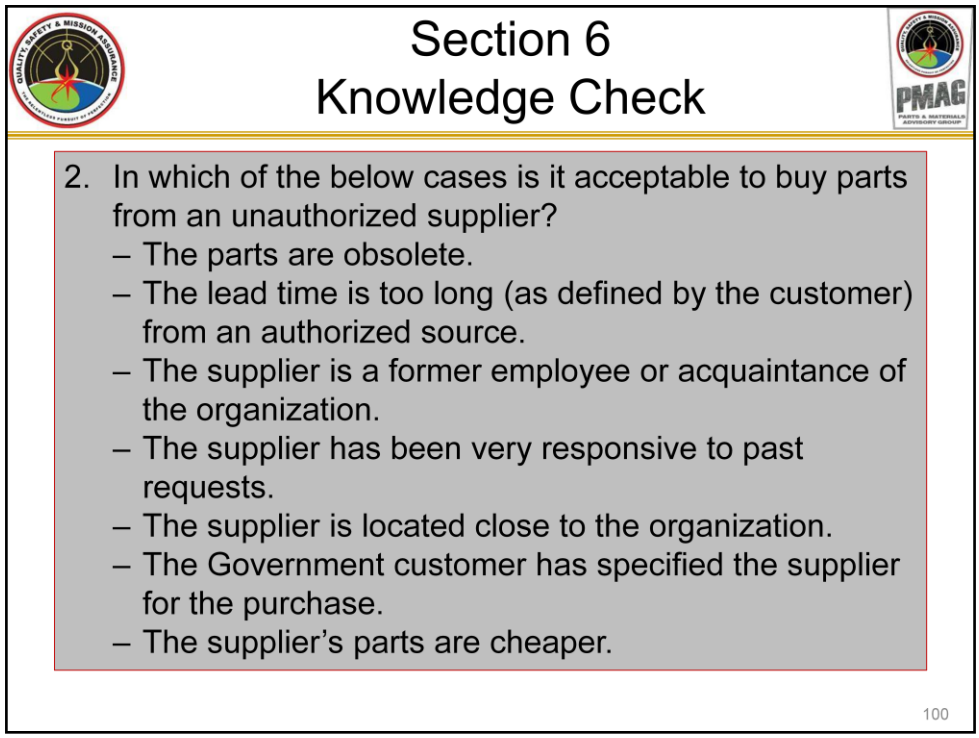
Shown on this slide are several contacts for notification about suspect or confirmed counterfeit parts or materials.



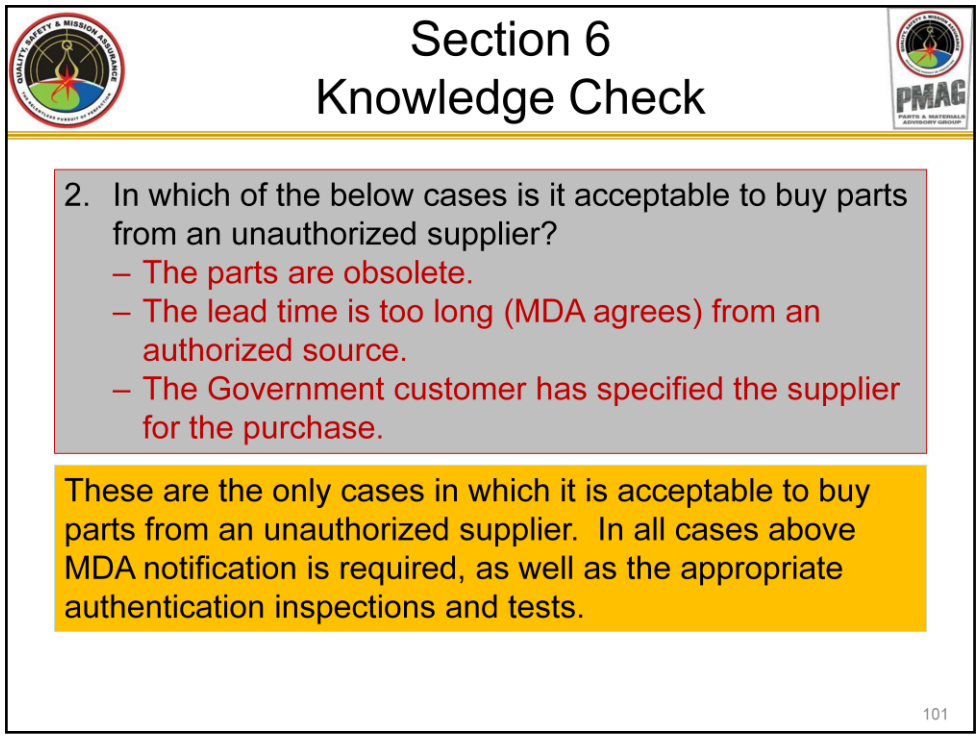
Test your knowledge of this section by reading each of the next seven questions. What is your answer for each one? Work your way through the next several slides to see how you did.



Before parts can be bought and installed in MDA systems, the contractor must notify MDA and the prime contractor by way of the Parts, Materials, and Processes Control Board, or PMPCB. Part of the notification includes justifying that an unauthorized supplier was the only viable option, providing any traceability available, and developing a plan for the inspection and test of the parts to the requirements of PMAP Table 5.

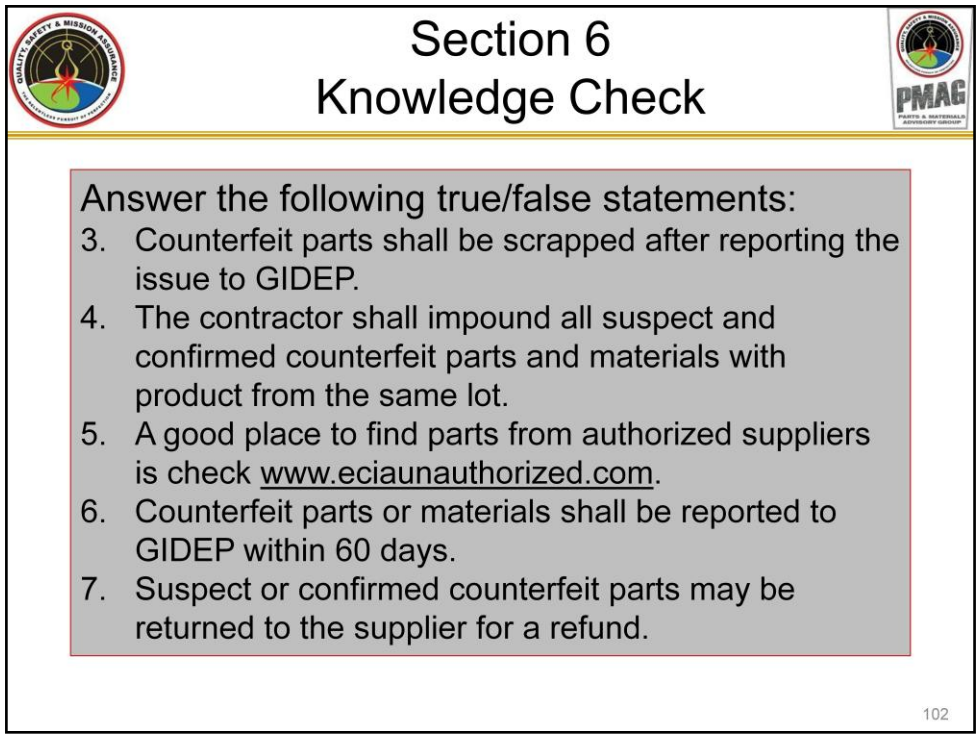


In which of the cases below is it acceptable to buy parts from an unauthorized supplier?

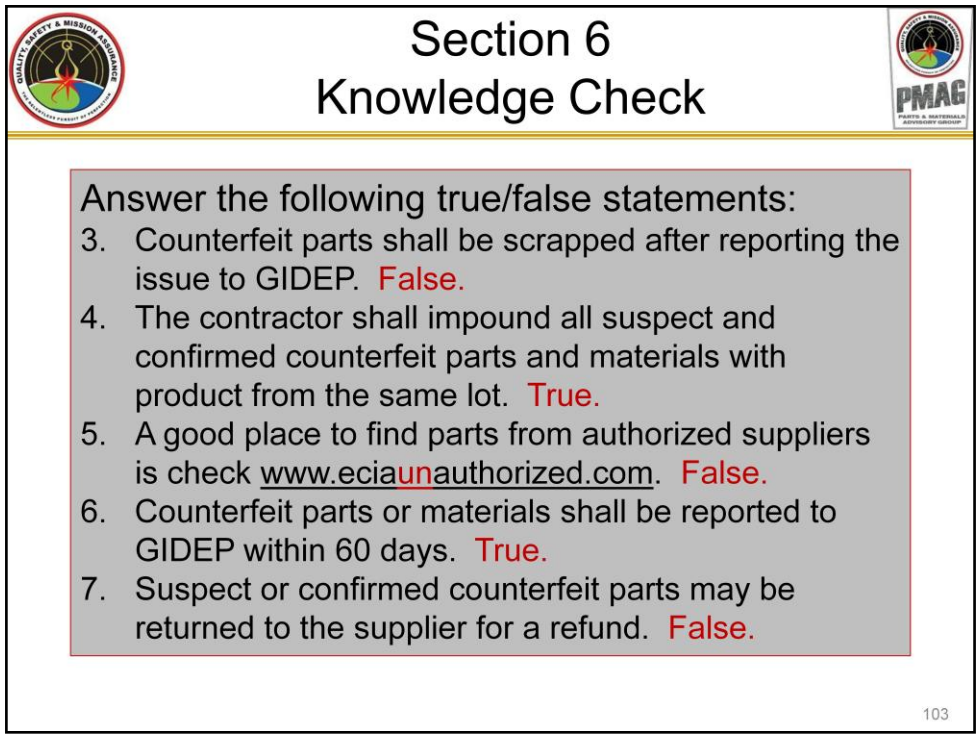


Electronic parts must only be purchased from unauthorized suppliers if there is no other legitimate choice. Obsolescence is the best reason. A long lead time might also be valid, as long as it is agreed to by MDA. There may also be times when the contractor's customer has directed a purchase from an unauthorized supplier. In all these cases, the contractor must still notify MDA via his customer and the PMPCB.

Other options, such as responsiveness, familiarity, and cost, are not valid reasons to buy electronic parts from an unauthorized supplier. In order to maintain system reliability, it is vitally important that Rule #1 be adhered to.



Answer the following true/false statements as a final test of your Section 6 knowledge.



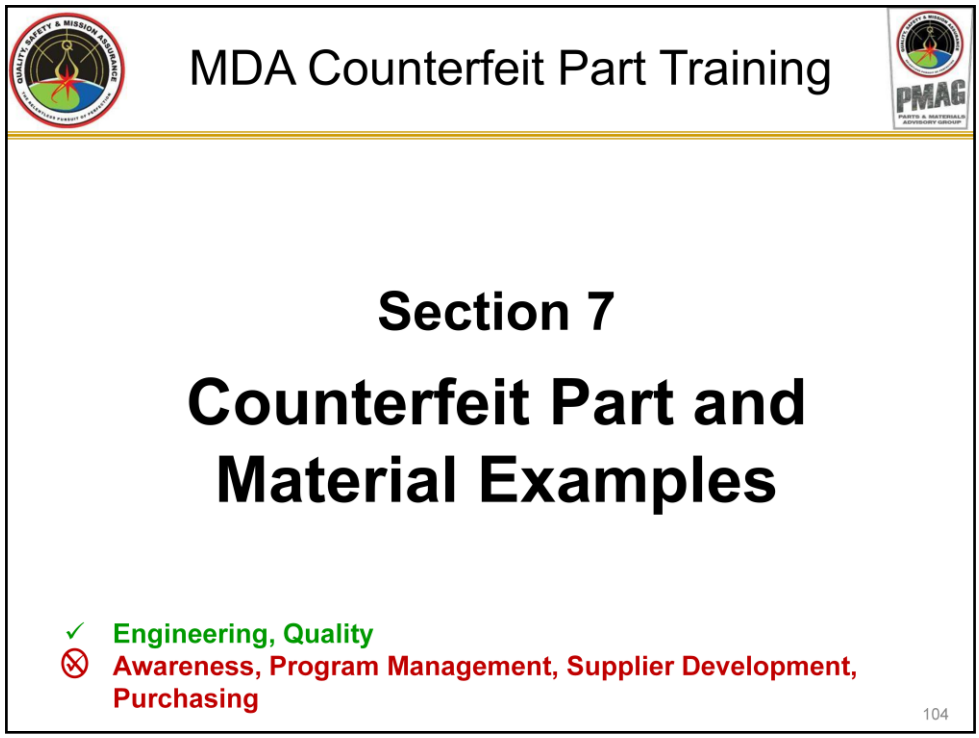
Statement 3 is false. Counterfeit parts cannot be scrapped without approval from MDA or investigative authorities.

Statement 4 is true. All suspect and confirmed counterfeit parts in the lot or date code must be impounded.

Statement 5 is false. The website is www.eciaauthorized.com, not eciaunauthorized.com.

Statement 6 is true. Counterfeit parts or materials must be reported to GIDEP within 60 days.

Statement 7 is false. Suspect or confirmed counterfeit parts may not be returned for any reason. Returned parts might be resold to another customer.

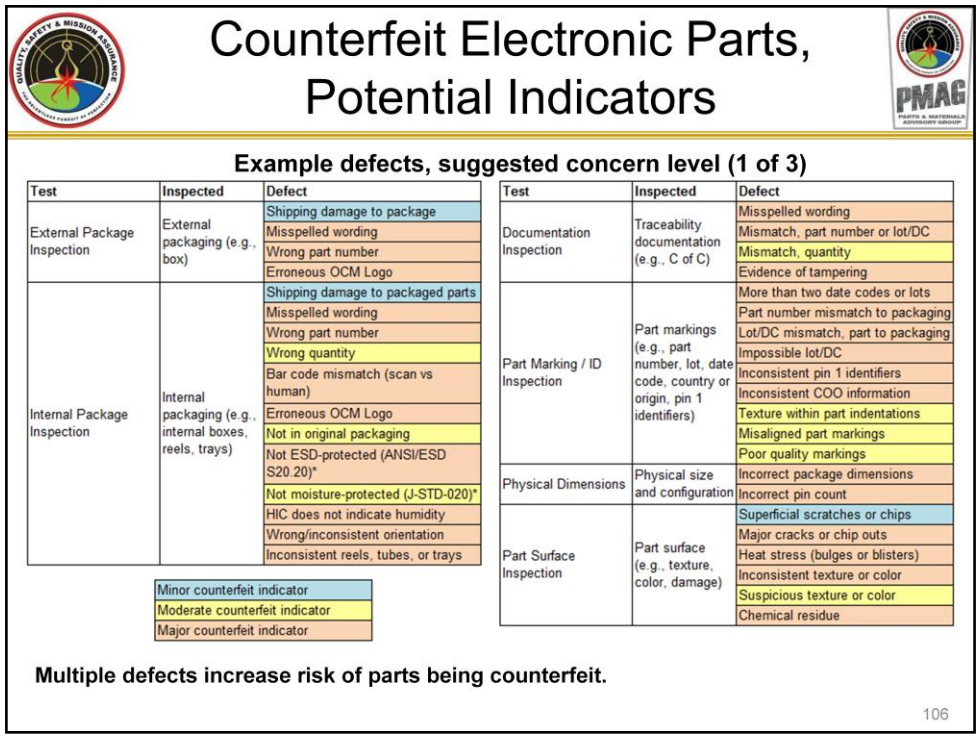


In this section you will find several examples of counterfeit parts and materials. These examples are all from GIDEP reports, or other Government and Industry information since 2012. Therefore, these represent the most recently discovered counterfeit parts and materials.

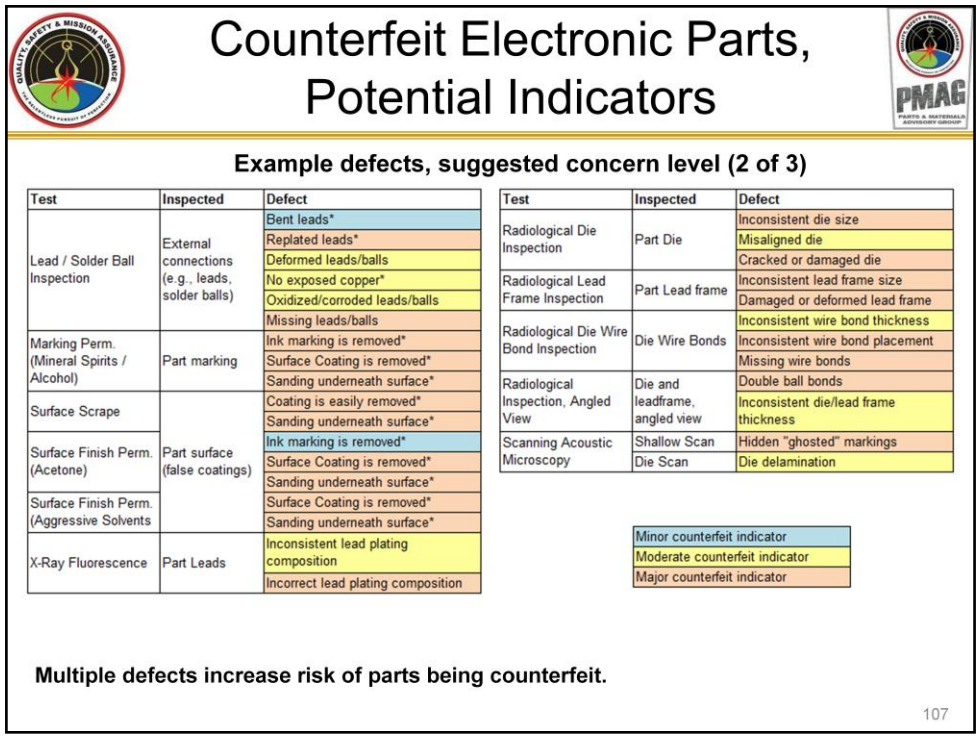
Detection Examples

GIDEP images removed – not for public use. Suggest GIDEP membership for excellent examples of counterfeit parts.

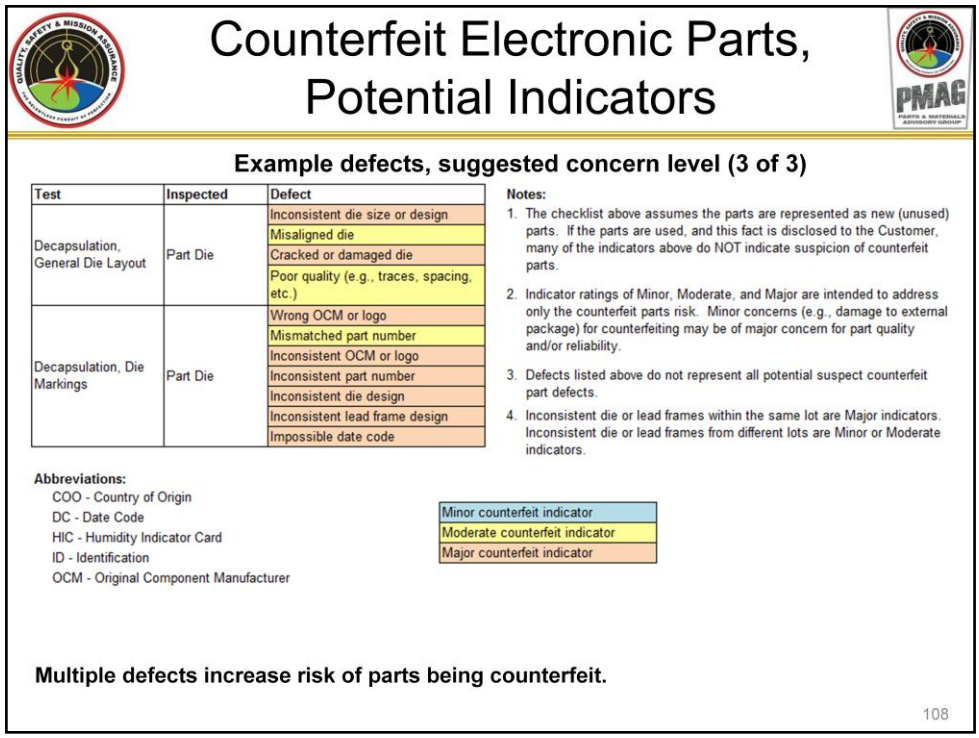
105



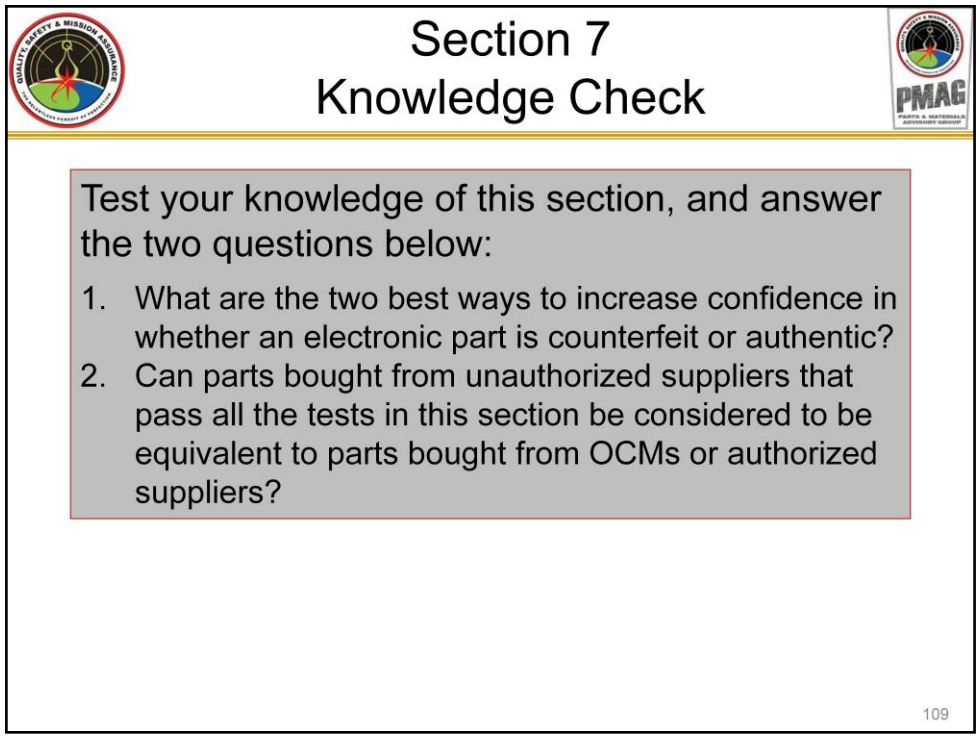
The information in the next three slides provides many potential indicators of a counterfeit electronic part, along with guidance on the importance of the indicator. Defects in orange shading are strong evidence of counterfeiting. All of the other defects may also indicate the part is counterfeit, but the confidence is reduced. A minor indicator for counterfeiting might still be a moderate or major quality concern.



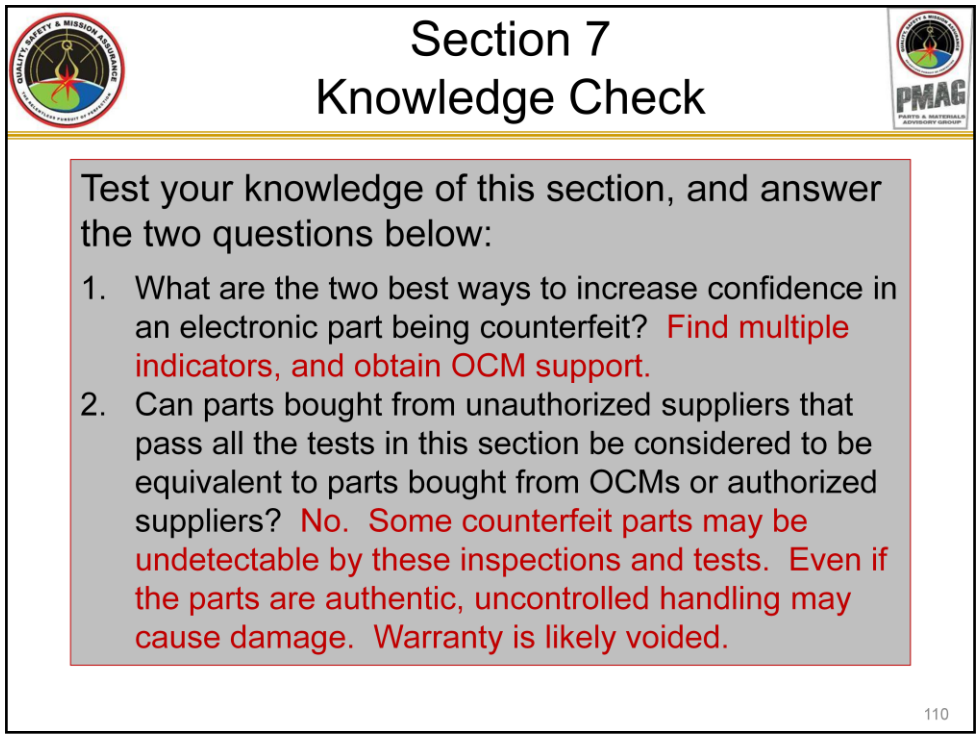
Here is the second slide on counterfeit part indicators. These indicators in concern levels were generated from information in IDEA-STD-1010B, GIDEP Alerts, and inputs from various DoD representatives. This should not be assumed to include all counterfeit indicators for electronic parts.



This is the final slide of indicators. Keep in mind that this assumes that the customer has requested new parts. There are many refurbished, or used, parts available in the open market. If they are not being sold as new parts they are not counterfeit, unless the parts have been misrepresented in other ways, such as wrong die, date code, temperature range, and so on.

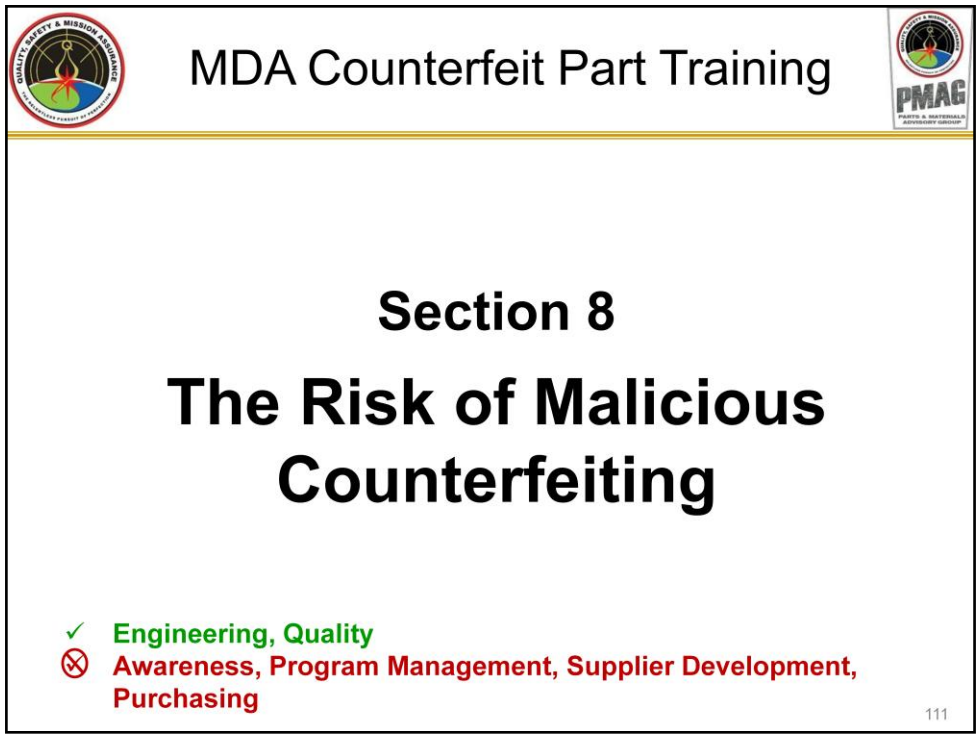


Test your knowledge of this section by reading each of the questions. What is your answer for each one? Go to the next slide to see how you did.



The two best ways to gain confidence that a suspect electronic part is indeed counterfeit are to detect multiple indicators during the inspection and test phase, and to obtain support from the OCM about the part's authenticity.

Parts bought from unauthorized suppliers should not be considered equivalent to parts bought from authorized suppliers or OCMs, even if they pass the inspection and test requirements. Even if the parts are authentic, the handling in the supply chain may not have been to industry best practices. In addition, the warranty may be void, since the parts were purchased outside the OCM's authorized supply base.



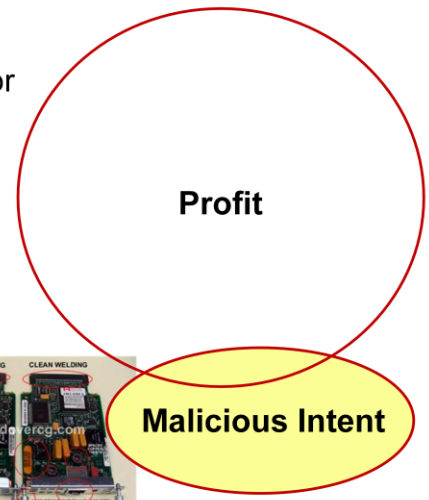
In this section you will learn about the risk of counterfeit electronic parts with malicious intent. There is potential for adversaries to tamper with or produce new parts that have embedded capabilities to potentially exploit the system.

Malicious Counterfeiting, Part Types

For Malicious Intent:

Parts critical to the system, or storing critical data

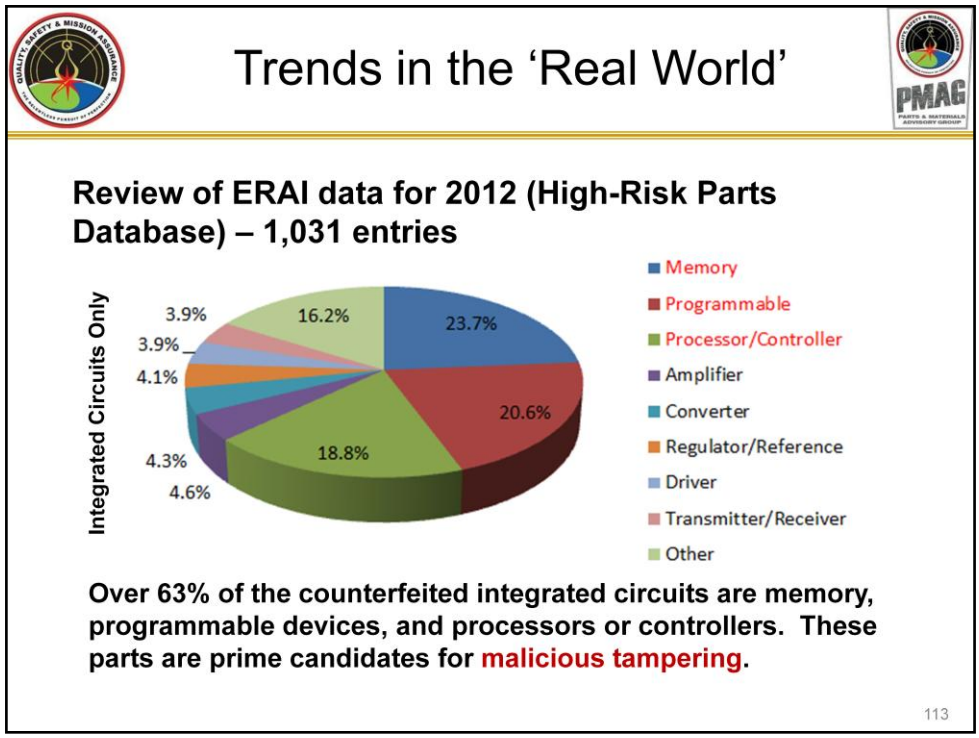
- Processors
- Programmable devices
- Military parts
- IT assemblies (computers, routers, network switches, etc.)



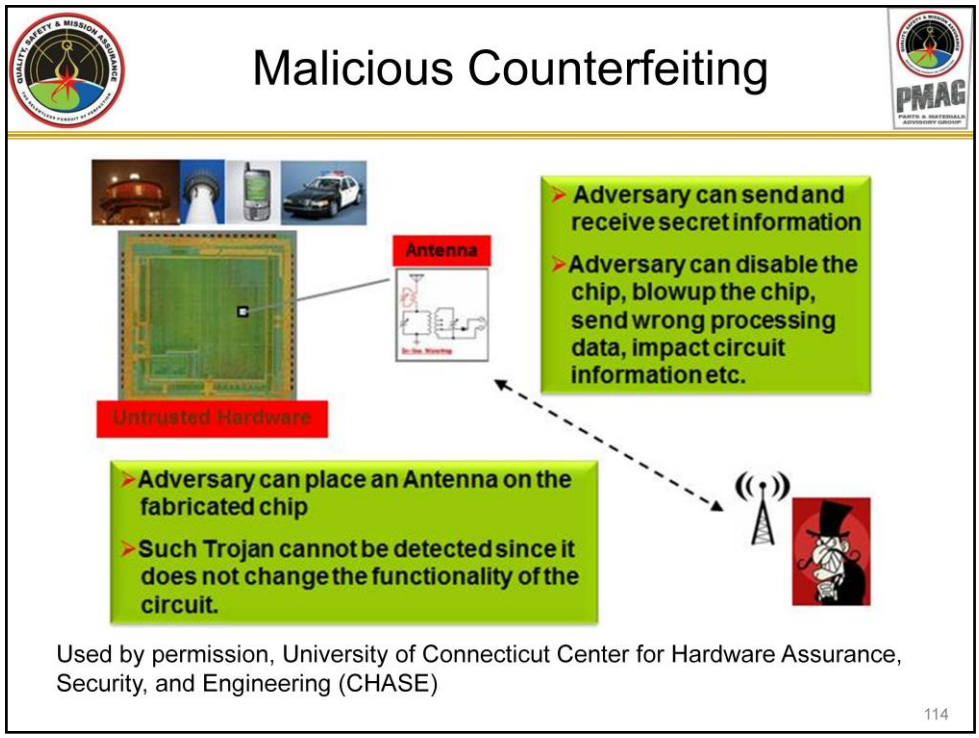
IT – Information Technology

112

While the majority of counterfeit electronic parts are produced and sold in order to make money, there is growing concern over the potential for parts to be altered, with malicious functions added. Critical military components like processors and field programmable gate arrays, or FPGAs, and also computers, routers, network switches and other information technology components are among the part types most susceptible to tampering. These parts, if counterfeited, might contain malicious codes or hardware that would potentially allow our adversaries to steal important data or disable our systems.



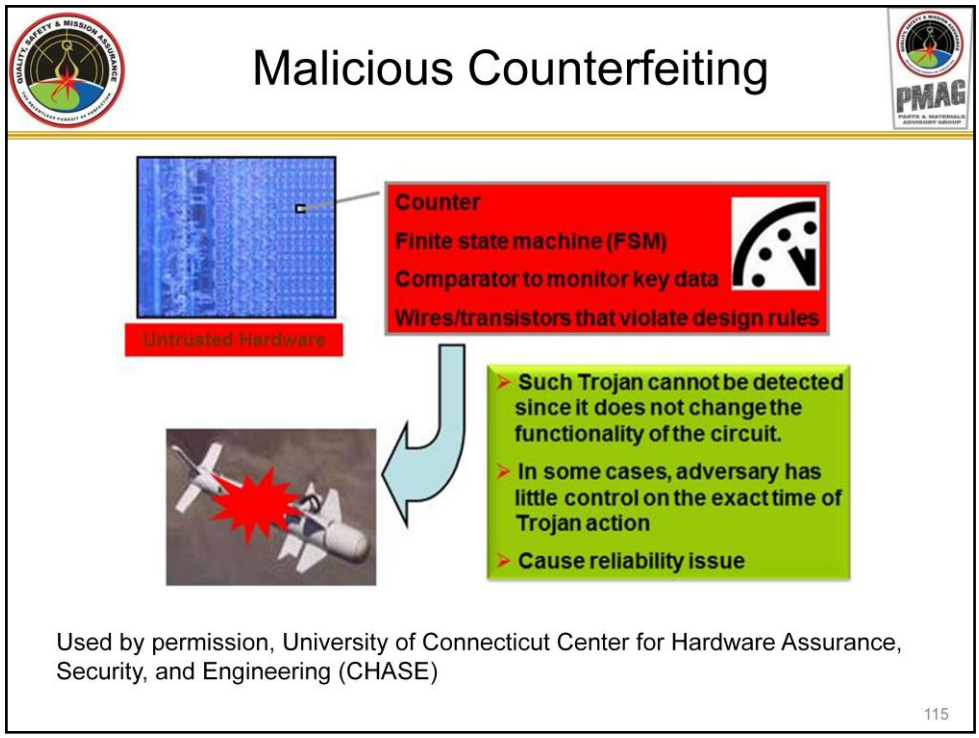
Of over 850 suspect counterfeit integrated circuits reported to ERAI in 2012, over 63 percent of them were either memory circuits, programmable devices, processors, or controllers. This is significant because these part types might provide the most value if an enemy wished to insert malicious code or circuitry into the part. These parts are the most likely to store critical system information, or be able to cause complete system failure if so desired.



This slide from the University of Connecticut's Center for Hardware Assurance, Security, and Engineering, or CHASE (pronounced 'chase'), shows how a critical part can be modified slightly, leaving very little visual evidence of the change. The part could then be called upon by our enemy to:

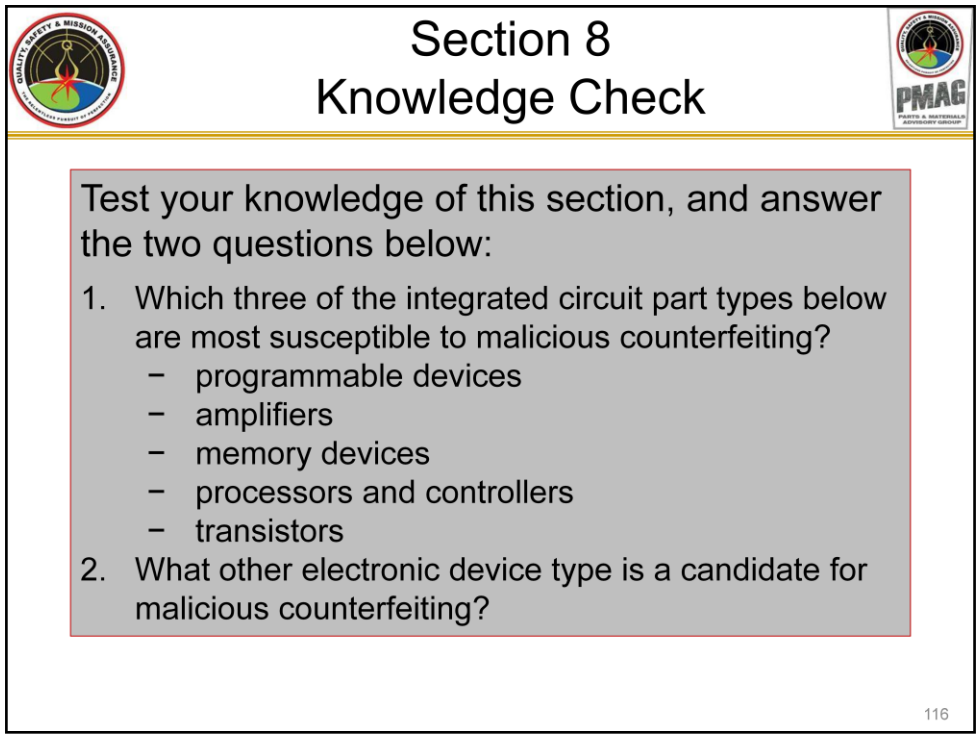
1. Monitor system information via an inserted antenna.
2. Send erroneous or malicious information to fool the system.
3. Cause the integrated circuit to fail or shut down, disabling the system.

Any of the possibilities above represent a serious breach of the integrity of a potentially critical system.

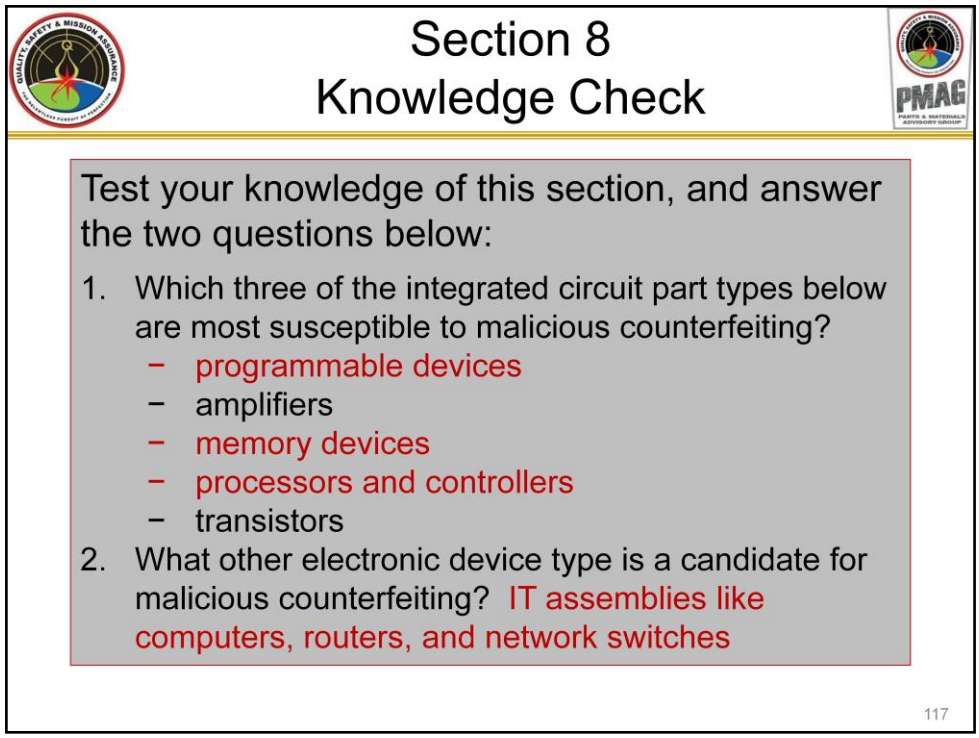


This additional slide from CHASE indicates that control over the 'destruct state' is likely to be limited. However, the part might be designed to monitor key events and data transfers, which increases the chances of shutting the system down during a critical activity.

Organizations like CHASE are currently actively working to develop tamper-proof methods for integrated circuits, including processes to detect changes to the part's die.



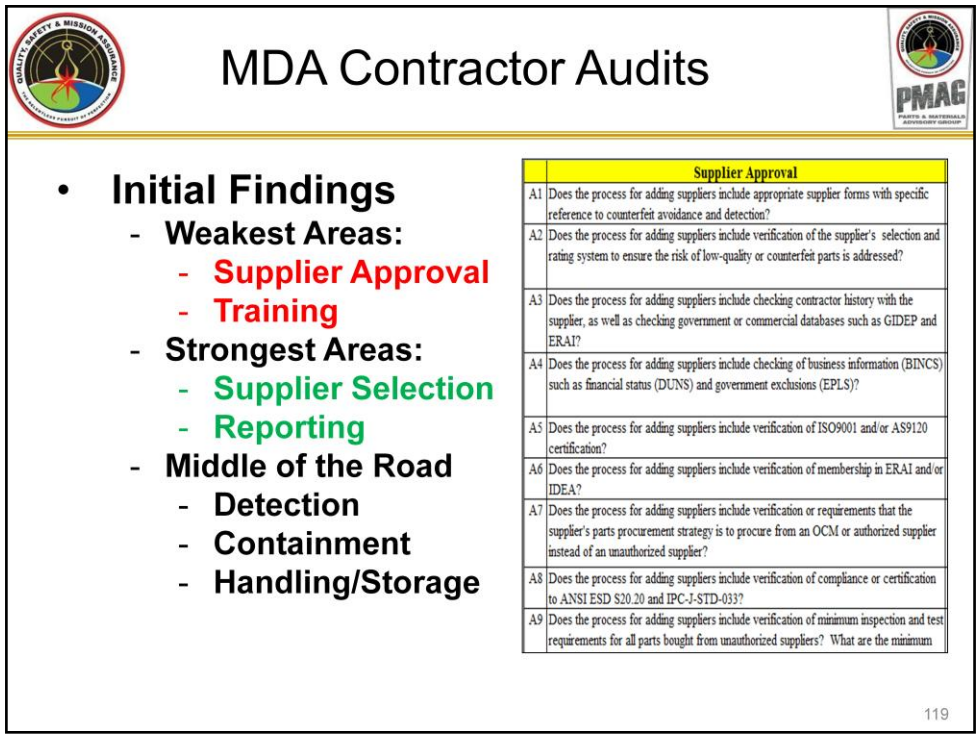
Test your knowledge of this section by reading each of the questions. What is your answer for each one? Go to the next slide to see how you did.



The three integrated circuit functional part types most likely to be tampered with maliciously are memory devices, programmable devices, and processors or controllers.

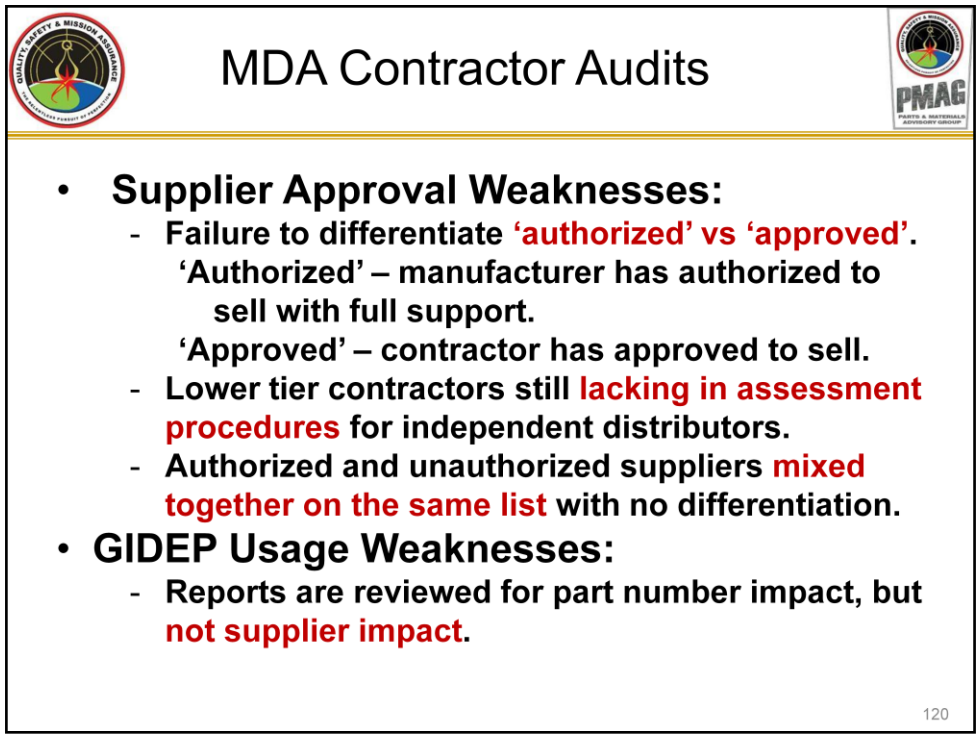
Additionally, information technology, or IT assemblies such as computers and other network assemblies are at risk if they are procured from unauthorized suppliers.

In this section you will learn about MDA contractor audits for counterfeit parts procedures, and what our contractors' strengths and weaknesses are.



MDA initiated enhanced contractor audits in 2012. Contractors had been undergoing MDA audits for several years, but MDA developed a 40-plus question checklist that allowed the auditor to generate a score for each of eight major anti-counterfeit areas, as well as an overall score. Each question can be scored from 1 to 5, with scoring guidance provided with the checklist. Use of this checklist in 2012 has identified several weaknesses in the MDA contractor supply chain for counterfeit electronic parts.

The primary weaknesses were determined to be Supplier Approval and Training. The rightmost image depicts nine questions from the Supplier Approval section as an example.

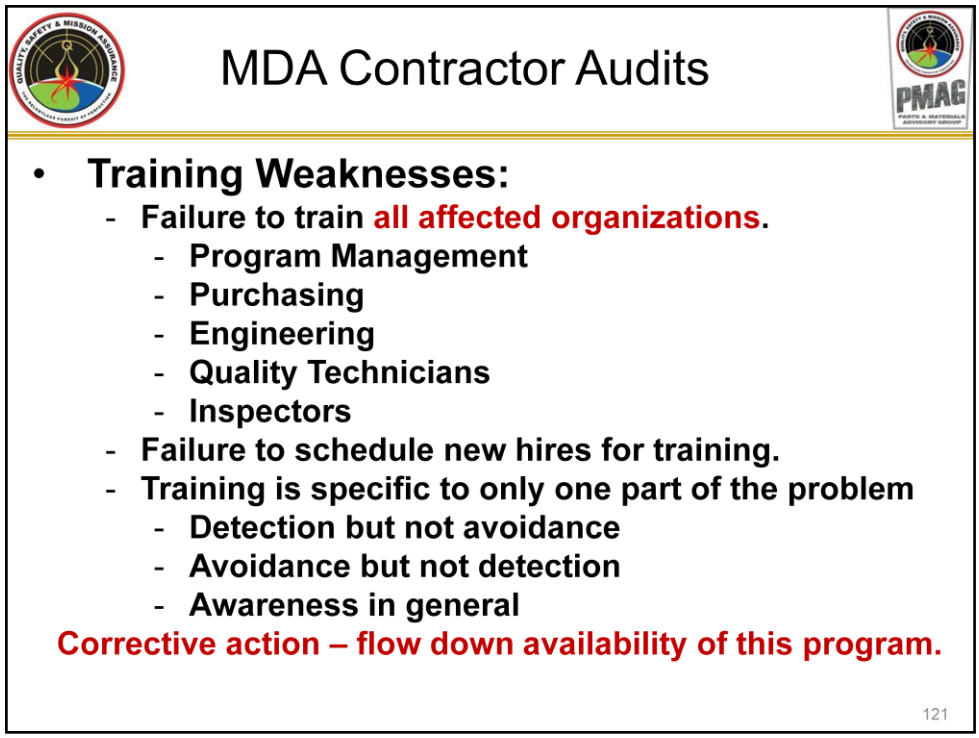


The most evident contractor Supplier Approval weakness was a confusion over the phrases 'authorized supplier' and 'approved supplier'. As MDA defines these, an authorized supplier is authorized by the OCM to buy parts directly, and sell them with full warranty. An approved supplier has been assessed by the contractor and approved to sell parts to the contractor. Considering an approved unauthorized supplier to be the same as an authorized supplier has resulted in contractors not informing MDA of unauthorized supplier purchases. This is a direct violation of both MDA's PMAP and Policy Memo 50.

We also found unauthorized supplier assessment procedures at the lower tiers to be lacking in detail to ensure the approved suppliers would be a low risk.

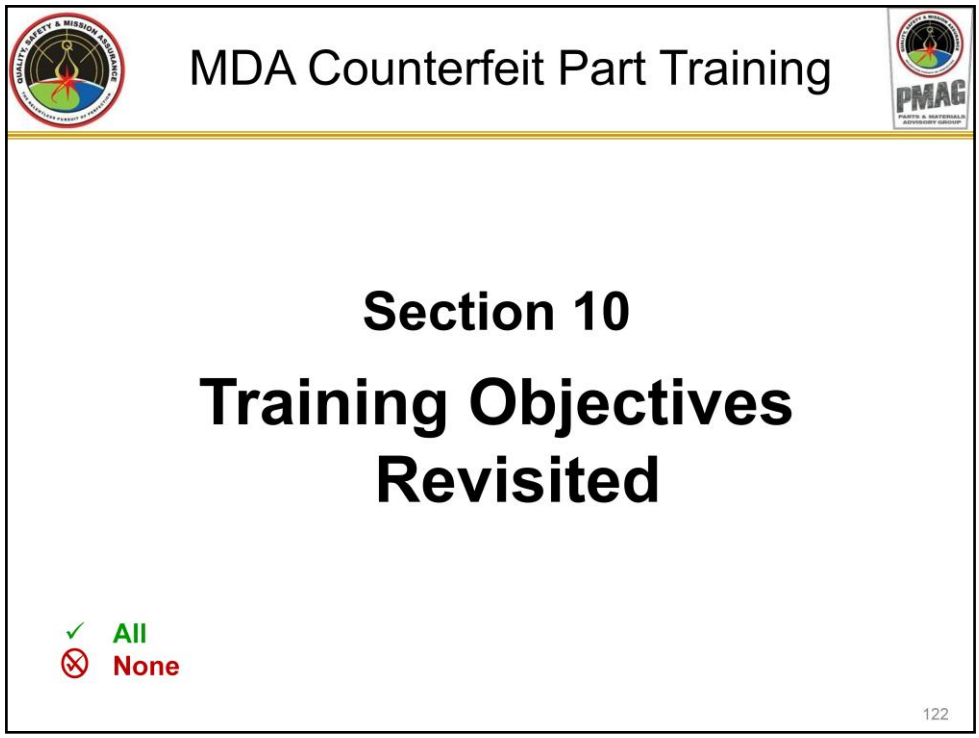
There is also almost universal mixing of authorized and unauthorized approved suppliers on the approved supplier listings. If the procedures are not specifically worded to force purchases from the authorized supplier first, there can be unnecessary purchases from approved, but unauthorized, suppliers.

Another comment mistake is that contractors are reviewing GIDEP reports only to see if the reported part is used within the facility. GIDEP reports should also be checked to see if the reported supplier is approved by the contractor, and if so, assess whether the supplier should be disapproved. In one case we found a supplier approved at a contractor facility, even though a different facility for the same contractor had identified serious concerns through GIDEP.

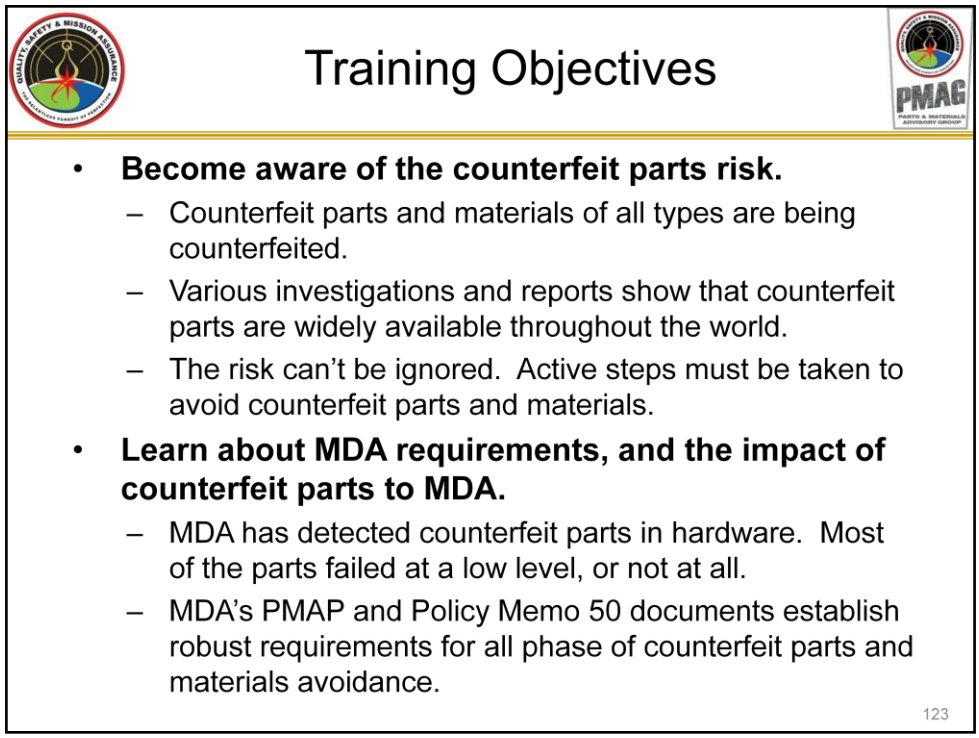


The other major weakness was in training. Smaller contractors do not have the expertise to develop a robust anti-counterfeit training program. The programs tend to be 'awareness courses' that do not go into sufficient depth to quantify the counterfeit risk to all affected parties such as program management, purchasing, supplier development, engineering, quality technicians and part inspectors.

Most of the training programs did not provide a broad immersion in all aspects including avoidance, detection, containment, reporting, and disposal. Therefore, this MDA program was developed as a standalone program that could be provided to MDA contractors to use as is, or to enhance existing programs.

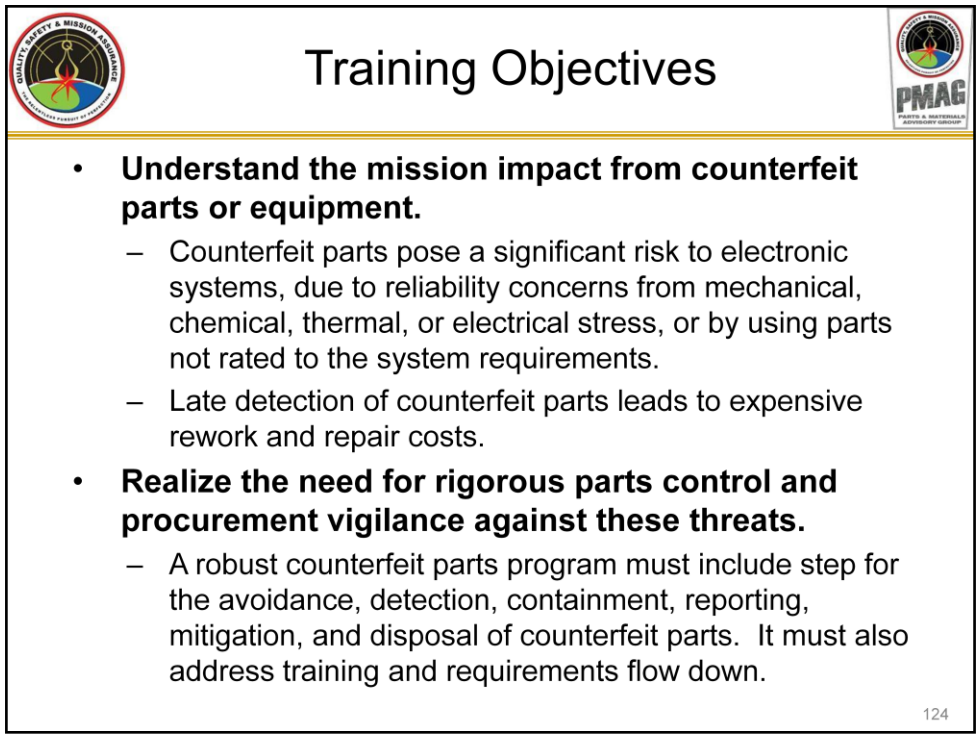


Let’s recap the training objectives for this course.



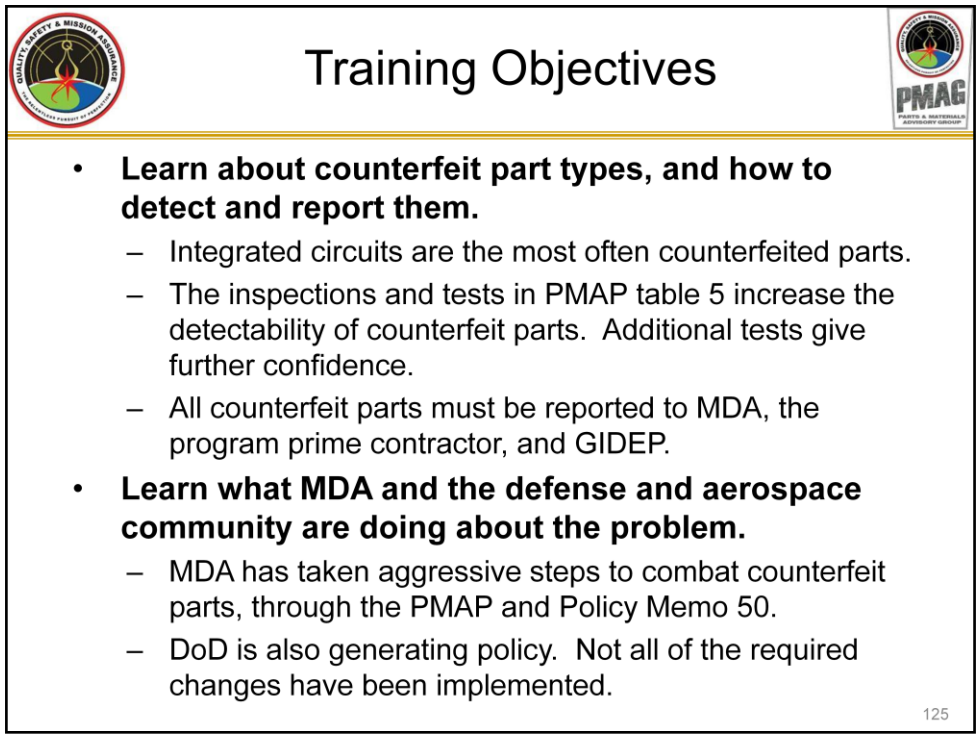
You should have learned that parts and materials of all types, from electronic parts to fire extinguishers to refrigerants, are being counterfeited for profit. Government and investigative reports have shown that counterfeit electronic parts are widely available throughout the world, and internet trading platforms make it easy to find them. The risk cannot be ignored. Only through the use of diligent and active steps can the risk be reduced to a manageable level.

Also, MDA has detected parts in system hardware, leading to expensive rework and repair in a few instances. Most of the detected counterfeit parts failed at a low level, or not at all. To help combat counterfeit parts and materials, MDA has developed the PMAP, and Policy Memo 50 documents, with a robust set of requirements for avoiding, detecting, containing, reporting, and disposing of counterfeit parts and materials.



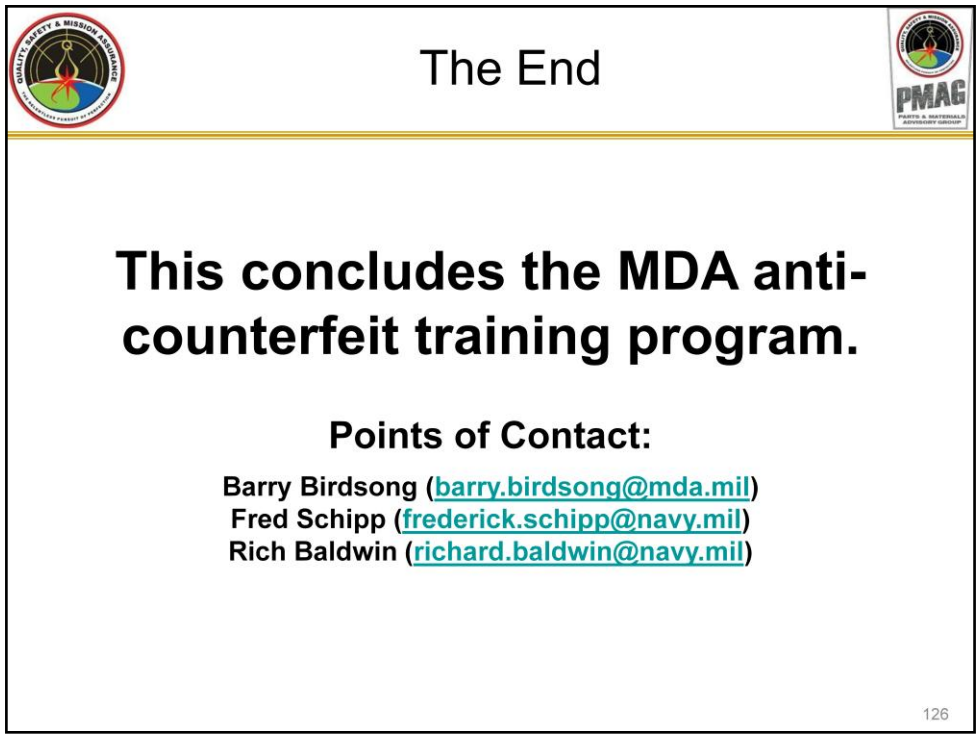
Counterfeit parts have likely been exposed to mechanical, chemical, thermal, and electrical stress during the removal, refurbishment, or reclamation of the parts. Or the parts may not have ever been tested to the system requirements. In both cases, this results in unreliable system performance. Late detection of counterfeit parts can lead to expensive rework and repair costs.

A robust counterfeit parts program must include steps for the avoidance, detection, containment, reporting, mitigation, and disposal of counterfeit parts. It must also address training and requirements flow down. Only by aggressively addressing all phases can the counterfeit parts risk be minimized.



Electronic parts are the most commonly counterfeited critical components. Of all electronic parts, integrated circuits comprise the lion's share of counterfeited parts. The inspections and tests required in PMAP Table 5 increase the detectability of counterfeit electronic parts, although additional tests can give even further confidence. All suspect and confirmed counterfeit parts must be reported to MDA and the prime contractor. A GIDEP report must be submitted within 60 days of detection.

MDA, DoD, and the aerospace community have taken active steps to combat counterfeit parts and materials. There is more policy in development by the Office of the Secretary of Defense in reaction to the National Defense Authorization Act of 2012. This policy should be released in 2013.



This concludes the Missile Defense Agency's anti-counterfeit training program. If you have comments or questions, please feel free to contact any of the names listed here. Thank you.

Appendix B. Best Practices and Lessons Learned

This appendix provides best practices and lessons learned from industry and government SMEs that have been intimately involved with the detection and avoidance of counterfeit electronic parts and the establishment of processes to prevent these parts from inadvertently getting into government products.

NOTE: Click on Link to see Best Practice/Lessons Learned Detail

B1: Reconstitute versus Redesign

Another approach to obsolescence management is to approach the OCM and ask if they would be willing to reconstitute a manufacturing/technology line. Example: On one satellite program two black boxes required obsolete microcircuits. The cost to the government for the OEM to redesign and requalify the black boxes was over $12 million. The government approached the OCM of that obsolete component and asked: "Would you be willing to reconstitute that component technology and what would it take (schedule and cost) to do it and by the way make it Class V and L-level Enhanced Low Dose Rate Sensitivity (ELDRS) qualified." In this case the OCM came back with a cost of $750,000 (NRE) and a unit cost of $350 per piece part. The lesson being, it cannot hurt to go back and ask the OCM for some help. (back)

B2: Check other Government Programs and Agencies for Excess Inventory

If a government program has a need for a EEEE part (whether obsolete or not) the needing contractor can request for their program office to query other programs offices if they have excess or available inventory. The NRO and USAF/SMC have a parts management tool that can used to query programs within their organization. The Parts, Units, Materials, Processes and Systems (PUMPS) tool is used to alert programs when failures, manufacturing, quality issues with parts, materials or processes are

identified by one program. The PUMPS tool can also be used to request parts availability from program's existing inventories.

For example, NASA Goddard Space Flight Center (GFSC) sent a request to the NRO when they had an immediate need for a voltage regulator because of a lot qualification failure at their supplier. GSFC was told that there would be a delay of about one year for them to get their parts. The NRO systems engineering directorate loaded the request into the PUMPS tool. As it turned out, one NRO program had excess inventory on the requested part. After some negotiations, the NRO was able to provide the quantity of parts needed by GSFC. The parts were delivered with the full data package and CoC. About one year later GSFC returned the parts when they received their part from their supplier. (back)

B3: Ensure Parts Inspected and Tested for Authenticity Prior to Shipment

Third party laboratory analysis verification of authenticity should be completed prior to allowing unauthorized supplier electronic parts to be received. The unauthorized supplier should be willing to ship the parts to a third party laboratory with inspection and analytical capabilities sufficient to ensure authenticity. Only after successfully passing these tests should the parts be conveyed to the user in order to ensure containment. (back)

B4: Categorize Your Suppliers and Train Appropriate Personnel

Consider identifying your electronic suppliers into three categories under your approved supplier list (ASL) and train Supply Chain Procurement personnel to look for these categories in the company ASL to reduce risk of ordering a counterfeit electronic part.

1. OCM. Little or no risk in using this type of supplier.
2. OCM Authorized Supplier. Little or no risk in the use of this supplier. Supply Chain will need to verify the supplier is an authorized supplier for this electronic part being procured.
3. Unauthorized Supplier. Very high risk. Supply Chain will need to let the program know this is high risk procurement and should have a risk mitigation plan for this electronic part.

The ASL should be separated between authorized and unauthorized suppliers. An ideal ASL would list which OCMs the suppliers are authorized to sell products for. Purchasing of parts from unauthorized suppliers should be impossible within the purchasing system (blocked electronically) without justification to and approval by management. The risks and potential costs should be specified when requesting management approval. (back)

B5: Use Cross-Functional Team When Developing Counterfeit Parts Prevention Strategy

Utilize a cross-functional team to develop your counterfeit parts prevention process, including legal representation. When developing your anti-counterfeiting processes, your team should be composed of personnel who have the most "real world" knowledge of how your company works. Given the economic consequences of delivering a counterfeit part, the best and most experienced personnel should be utilized. (back)

B6: Understand Lower-Tier Supplier Risk Tolerance Level

In order for prime or upper tier contractor to perform a meaningful product assurance and end item performance risk assessment, the contractor should have visibility into how its subcontractors apply risk assessment approaches. The key is understanding the lower-tier supplier approach to countering the risk of procuring counterfeit parts. This understanding provides the opportunity for the prime or upper-tier contractor to establish controls to ensure their risk tolerance level is met. Without this visibility, the prime or upper tier contractor is left with a "faith-based" risk assessment. (back)

B7: Establish Known Inspection/Test Requirements and Ensure Understanding

Some contractors require inspection/test from distributors or labs before accepting parts bought from unauthorized suppliers, but the quality/engineering personnel are not familiar enough with counterfeit part detection to know if the resultant report has adequately checked the parts for authenticity. To alleviate this a contractor should establish a known listing of inspection/test requirements, as well as a report format (checklists, photos, etc.) that allows adequate review. This could be a process where:

- Inspection/test requirements are documented and available to persons reviewing the data/reports.
- Test report template/guidelines are developed to help minimize variability and ensure the consistency and quality of test reports.
- The number of sources approved to conduct counterfeit inspection/test tasks is minimized.
- Test reports are thoroughly reviewed by persons knowledgeable in:
  - The commodity being evaluated
  - Counterfeiting techniques
  - Methods of counterfeit detection
  - Industry and or company specific definitions/criteria for classification of items as counterfeit/suspect counterfeit (back)

B8: Remain Diligent When Electrical Test Failures Encountered

Failure analysis of electrical test failures should include an automatic check of whether the identified failing part was bought from an unauthorized supplier. Additional questions are required if the purchase was from an unauthorized source to determine if the part is authentic. (back)

B9: Additional Actions Required When Electronic Parts Receive Value-Added Service

Original OEM/franchised distributor parts that go through any valued added service company (e.g., test house, solder dipping, IC PROM programming house) should go through additional testing and verification when received by purchaser to ensure no part substitutions occurred. (back)

B10: Include Check of Approved Supplier List When Evaluating GIDEPs

Contractors may not generally check GIDEP counterfeit part alerts to determine if the reported supplier is currently approved by the contractor. They check manufacturer, part number, and lot/date code, but if there is no match, often nothing is done – the contractor ignores the fact that one of its approved suppliers may have just been reported for selling counterfeit parts. GIDEP search processes should include checking the reported supplier against the contractor's ASL. If there is a match, the supplier should be contacted and requested to describe its corrective and preventive actions or refute the report. If the

contractor is unable to confirm the supplier has adequate counterfeit prevention processes, the supplier should be removed from the ASL. (back)

B11: Investigate All Parts Received from Supplier When Evaluating GIDEPs

When investigating usage for a reported counterfeit incident (GIDEP), do not focus on just the part number mentioned in the GIDEP. The investigation should determine if any part was received from the supplier noted in the GIDEP, not just the part number(s) noted. If one counterfeit part passes through a supplier's processes, others may have as well. Evaluating any and all usage of a supplier may provide early detection of other incidents and enable more proactive resolutions, even if subsequent GIDEPs are issued against this supplier. (back)

B12: Perform Due Diligence Before Tailoring Terms and Conditions

Allow minimal deviations to your Terms and Conditions, you will ultimately become liable. The present legislation contains severe financial penalties for delivering counterfeit parts to the government. Do not tailor your rights away by accepting more of the financial burden/liability. Always consult Legal consul. (back)

B13: Understand Requirements of Quality Clauses and Terms and Conditions

Have a clear understanding of the Quality Clauses/Terms and Conditions. When your customer applies Quality Clauses/Terms and Conditions related to counterfeiting, you need to understand and comply with them. If you have a question you need to go back to your customer for clarification. If you can't comply you need to inform your customer immediately. Ignorance of these contractual requirements or government regulations could have dire financial consequences for your company. (back)

B14: Drop Shipping Requires Additional Coordination

Establish a process when drop shipping of products is required. Drop shipped goods present a challenge since an unbroken chain of traceability (i.e., visibility to every intermediary in the supply chain) for each shipment is a requirement of DFARS 252.246-7007(c)(4). This more than likely will require special handling and coordination between the organization and it's supplier. (back)

B15: Know When "Return" Parts are Being Received

Include a clause in the purchase order that authorized and approved suppliers shall notify the purchaser if parts ordered are a "return." If they are a return, then additional testing would be required to ensure parts were not remarked and die is authentic (typically via DPA and die comparison). (back)

B16: Provide Adequate Training Program for Lower-Tier Supplier Use

The higher tiers, or DOD/aerospace should provide an adequate training program to the lower tiers for use. Lower tier contractors may not have the higher level knowledge of counterfeit parts, or the funding to learn counterfeit parts well enough to develop an adequate training program at their own facility. Counterfeit training generated by a small company (less than 500 people) is likely to concentrate primarily on buying from authorized suppliers and calling out AS5553. It will often lack counterfeit examples, military/customer requirements, guidelines for assessing suppliers, knowing the difference between authorized and unauthorized suppliers, etc. Appendix A of this guidebook provides examples of training programs. (back)

B17: Ensure Timely Training of Appropriate Personnel

Train as soon as possible, do not delay. Get the word out early and often regarding the importance of your anti-counterfeiting processes. Train all relevant personnel, such as: Design Engineers, Procurement Personnel, Quality/Receiving Inspection, Program Management, and Legal representation. (back)

B18: Perform Periodic Assessments of Counterfeit Parts Process

If you think your process is bullet proof, think again. Do not assume anything, question everything. Once your process is established, and up and running, perform a detailed audit to verify that the process is actually working. Examine samples of purchase orders to be sure that the parts being bought are truly coming from an authorized supplier. This needs to be part of your internal audit process and evaluated on a regular basis. Ensure your process is working; then, if you ever have an incident you can demonstrate it wasn't neglected. (back)

B19: Clearly Define Terms and Definitions

Have clear and unambiguous definitions. Terms like approved supplier, OCM, OEM, authorized supplier, unauthorized supplier, need to be clearly defined and understood. Personnel in different organizations will have a different understanding of what a term will mean. Example: An "approved supplier" in a Quality database may only be based on the supplier's quality rating or quality systems approval, not that this supplier is an OCM authorized source of supply. An "approved supplier" in a procurement database could have an entirely different connotation. All of these systems need to be consistent in defining terms and expectations. (back)

B20: Maintain Currency and Knowledge of Counterfeit Legislation

Become knowledgeable in the status of current legislation. The law on this subject is new and growing. The DFARS was released on May 16, 2014. These new laws and regulations WILL affect your business. Obtain legal counsel; ignorance of the law will not be an acceptable excuse if there is a counterfeit part incident with your company. (back)

B21: Retention and Control of 'Gold Standards'

'Gold standards' are a major tool for identifying if a part is likely to be counterfeit. In some instances the nameplate manufacturer (i.e., the manufacturer whose name and/or logo is marked on the part or the accompanying documentation) is either not available to assist in identifying part authenticity or is uncooperative. A good practice is to maintain and control detailed information on known good electronic part information from each manufacturer. This may include known good part samples, images, dimensions, performance curves, materials analysis, etc. (back)

Appendix C. Observations and Driving Philosophies

This appendix provides observations and philosophies from industry and government SMEs that have been intimately involved with the detection and avoidance of counterfeit electronic parts and the establishment of processes to prevent these parts from inadvertently getting into government products.

NOTE: Click on Link to see Details on Observations and Driving Philosophies

C1: "Trusted" Suppliers

Section 818 of the FY2012 NDAA uses the term trusted supplier. This terminology is not used in the DFARS rule and is not used in this guide. Its use in the NDAA differs significantly from its current use with respect to the "DOD Trusted Foundry Program,"[31] an accreditation plan for design, fabrication, packaging and test services across a broad technology range for specialized governmental applications. In the context of counterfeit part avoidance, use of the term trusted supplier should describe a preference for the use of an authorized supplier and include suppliers who obtain electronic parts exclusively from authorized suppliers. (back)

C2: Independent Distributors and Brokers

Independent distributors are not all created equally. Some independent distributors have demonstrated capabilities and standards of ethics above others. Some are members of various industry organizations supporting the independent distributor market. Some have pursued certifications to various product quality related programs (e.g., AS9120, CCAP-101). Even with these credentials, independent distributors and brokers are not authorized nor do they generally have the ability to verify the authenticity of products they sell.

[31] https://dap.dau.mil/career/log/blogs/archive/2012/01/24/dod-trusted-foundry-program.aspx

For example, independent distributors and brokers are not well poised to:

- Certify compliance to manufacturer specifications or US government specifications (e.g., MIL-PRF-38535 QML product)
- Verify traceability to the original manufacturer
- Demonstrate that parts have been properly handled and stored by other supply chain intermediaries
- Perform inspections and tests needed to provide sufficient product assurance for many defense and aerospace applications. (back)

C3: Considerations When Using A Contract Manufacturer (CM), Electronic Manufacturing Service (EMS), Or Third Party Logistics Provider (3PL)

Some electronic equipment developers outsource manufacturing services to a Contract Manufacturer (CM), Electronic Manufacturing Service (EMS), Third Party Logistics provider (3PL) or Value Added Service provider. The term "CM" or "EMS" generally refers to an organization that manufacturers products developed by others. Prominent examples include Foxconn Technology Group and Pegatron Corporation who produce iPhones and iPads for Apple Inc. Some CMs perform "consignment manufacturing" where a product developer outsources the assembly of its products, but maintains direct control over some portion of the overall manufacturing supply chain in-house, such as materiel procurement and system level assembly. Other CMs offer "turnkey manufacturing" services which perform all manufacturing functions, including material procurement, inventory control, receiving, and kitting. A "3PL" or "Value Added Service provider" performs part or all of a customer's supply chain management functions. These services can also include value-added services related to the procurement of materiel and preparing materiel for assembly manufacturing (e.g., testing, packaging, termination resurfacing, etc.).

Some turnkey manufacturing companies 3PL, and value added service providers also function as an independent distributor or have established a formal partnership with an independent distributor. The selection of these services should include a review of purchasing practices, material control and materiel transfer practices to identify potential vulnerabilities to counterfeit electronic parts. (back)

C4: Considerations When Partnering With Small Business

Why would one use other suppliers when parts are currently produced by and available from an authorized supplier? U.S. government agencies, including the DOD, flow down expectations to enhance subcontracting opportunities for small and small disadvantaged business concerns. One method that contractors use to be responsive to these expectations is to outsource part procurement to small and small disadvantaged businesses. Section 818 of the FY2012 NDAA supports this approach. Referring to Section 818(c)(3)(A), DFARS rule 252.246-7007 (c)(5) requires the "use of suppliers that are the original manufacturer, 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. When parts are not available from any of these sources, use of suppliers that meet applicable counterfeit detection and avoidance system criteria." The DOD and its contractors should recognize, however, that counterfeit electronic parts tend to enter the supply chain through independent distributors and brokers and many independent distributors and brokers are small or small disadvantaged businesses.

When selecting small and small disadvantaged businesses to be suppliers of electronic components, the DOD and its contractors should flow down requirements to small and small disadvantaged businesses directing procurement from an original manufacturer or its authorized dealer. In cases where a contractor considers the use of small and small disadvantaged businesses to acquire electronic parts that are not available from an original manufacturer or its authorized dealer, the buyer should ensure effective counterfeit avoidance, detection, and risk mitigation processes are in place or apply significant oversight to ensure the authenticity of parts. (back)

C5: Obsolescence Management And Its Relationship To Counterfeit Electronic Part Avoidance

Defense and aerospace products are particularly vulnerable to counterfeit parts due to part 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. While changes to procurement practices will reduce the number of purchases from higher risk suppliers, the prominence of through-life support contracts will make part obsolescence a larger challenge and counterfeits a possibly bigger problem for DOD and defense companies in the future.

Obsolescence management and its relationship to counterfeit electronic part avoidance is generally known to DOD and it contractors. It has been a prominent topic at DMSMS & Standardization conferences for the past several years. Training and awareness programs established by the Defense Acquisition University describe the relationship between obsolescence management and counterfeit electronic part avoidance. A presentation by the U.S. Navy at the December 2008 public meeting on FAR Case 2008-019, Authentic Information Technology Products, included a discussion on this topic. It was also discussed extensively during the November 2011 U.S. Senate Armed Services Committee Hearing to receive testimony on the Committee's investigation into counterfeit electronic parts in the DOD supply chain. In order to reduce the likelihood of having to purchase parts through riskier supply chains, 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 often constrained regarding their ability to support and fund approaches to eliminate the use of obsolete components.

When assessing product offerings and proposals for production and support contracts, seek out information concerning the potential demand for obsolete parts associated with the product offering. Assess plans to either assure authorized sources of supply for obsolete electronic parts, or plans to implement design modifications to eliminate obsolete electronic parts. (back)

C6: Controlled Maintenance and Repair Operations - What Is Not A Counterfeit Electronic Part?

A significant number of counterfeit part discoveries involve parts that were used, but represented by the supplier as new and unused. Forensic analysis of several examples show evidence of termination refurbishing and reclamation; many also exhibited other indications of damaging exposures and included disguises intended to deceive a buyer. Exposures during counterfeiting operations can damage the components and can cause them to fail in use.

In contrast, controlled maintenance and repair operations do not subject parts to the abuse associated with e-waste feedstock for counterfeiters. Quite the contrary, these operations apply precautions to avoid damaging parts. In the case of DOD depots and contractor operated rework and repair facilities that apply reclamation practices (where parts are salvaged from used assemblies), this is generally done as a last resort to fill critical supply shortages and with full knowledge of the end customer. Though there may be a degree of concern with respect to reliability (after all, these parts have seen some amount of operation

and, therefore, their service life is reduced), controlled maintenance and repair is a necessary and well understood practice. (back)

C7: Counterfeit Detection Through Inspections And Tests Conducted By Independent Distributors

Despite the inspection and testing protocols applied by independent distributors and brokers, counterfeit products have escaped detection and were first identified to them by their customers. Inspections and tests performed by independent distributors tend to include low cost and expedient techniques that reveal easily detectable counterfeits. More rigorous, costly and time consuming methods are necessary to (1) detect more subtle variants of counterfeiting that can affect performance in the end use application, and (2) reveal defects from damage induced by inadequate handling and storage, termination refurbishing, or reclamation. Many parts acquired from independent distributors may have started life as authentic parts, but show evidence of poor storage and handling conditions, or evidence of termination refurbishing or reclamation.

Close examination of the GIDEP reports reveals that the testing and inspection approach applied by the independent distributor did not include important methods, particularly the more rigorous, costly and time consuming methods that have greater potential to detect more subtle variants of counterfeiting that can affect performance in the end use application and defects from damage induced by inadequate handling and storage, termination refurbishing, or reclamation. Examination of the GIDEP reports reveals other examples where the supplier was not applying methods to counter newer and more advanced counterfeiting techniques discussed at various industry conferences, symposia and training programs available to independent distributors and brokers.

Existing standards commonly used by independent distributors may only specify minimum tests and inspections based on the limited capabilities of most independent distributors. These minimum required tests and inspections, however, may not provide sufficient due diligence and product assurance needed for defense and aerospace applications.

Mature industry and government inspection and test methods were designed to verify the integrity of authentic parts … not to detect counterfeits. Test protocols offered by suppliers may not detect damage associated with used parts. While adjustments to and combinations of these methods can detect suspect counterfeits, they are not foolproof.

Individual methods may not definitively distinguish authentic parts, or detect damage induced by inadequate handling and storage, termination refurbishing, or reclamation. A suite of inspections and tests are necessary to detect counterfeits and eliminate infant mortality defects, and to establish high level of confidence of failure free performance and to support an assembly/system level reliability assessment.

Documentation provided by an independent distributor or broker may not be authentic. Cases have been reported where forged documents were provided by independent distributors as evidence that parts sold were authentic and to provide traceability to the OCM. Examples of such documents include certification documents, traceability documentation, and test reports. (Reference Case Study #2)

Users should either acquire or consult subject matter expertise necessary to interpret documentation and assess the technical merits of inspection/testing protocols offered to detect counterfeits, and to assess the results of forensics and tests. (back)

C8: Counterfeit Detection Through Inspections And Tests Conducted By Independent Test Laboratories And Material Analysis Facilities

Test and material analysis laboratories are accustomed to evaluating compliance to mature industry and government standards and specifications. When selecting independent test laboratories and material analysis facilities, assess their subject matter expertise in conducting inspections and tests specifically designed to detect counterfeits and in analyzing the results of these inspections and tests.

SMEs in failure analysis and counterfeit detection conducted a round robin technical evaluation of several independent test labs to assess the ability of these laboratories to identify counterfeit devices and specific counterfeit attributes. Each lab was provided counterfeit and authentic samples of microcircuits. Each lab was encouraged to apply its standard counterfeit detection flow and requested to perform an assortment of specific tests and inspections commonly used for counterfeit detection. Laboratory results were compared to results from the aerospace electronics industry representative's analysis; where results differed, the representative's results were validated.

Observations from this round robin evaluation include the following:

- A significant variance was observed in the depth of analysis performed by each lab as well as variances in the fidelity of performed tests between labs.
- The training level and understanding of counterfeiting techniques of operators varied; a general lack of standardized certification was observed. The SME offered a compelling observation associated with these findings: "analysis isn't about performing a defined process; it is based on interpretation of observations. It is very difficult to standardize accreditation in this area."
- Poorly reported data can provide misleading conclusions; conclusions are not always well supported by the lab reports.

When outsourcing counterfeit detection activity, buyers should be specific concerning tests and inspections to be performed, oversee detection testing and analysis reporting, and consult SMEs on the results of detection testing and conclusions from analysis results. When assessing supplier and subcontractor expertise, (1) monitor the selection and specification of tests and inspections necessary to detect counterfeit parts, and (2) oversee execution of counterfeit detection testing, and the assessment of third party lab test results. (back)

C9: Revealing Disguises And Damage

When investigating counterfeit parts findings in the 2007 timeframe, industry SMEs observed that a significant number of these cases involved parts that were used, but represented by the supplier as new and unused. Forensic analysis of these parts showed evidence of termination refurbishing and reclamation; many also exhibited other indications of counterfeiting. When devising a counterfeit detection protocol, these SMEs selected tests that would reveal disguise techniques used by counterfeiters, but also included tests better suited to revealing defects from damage induced by abuse and contamination associated with counterfeiting operations – excessive heat, moisture, contaminants, electrostatic discharge and the combinational effects of these exposures. The tests and inspections selected to reveal this sort of damage included electrical testing, thermal cycle testing, fine and gross leak testing (for hermetic devices), and burn-in.

Since devising this process flow, more sophisticated counterfeit detection methods have been developed in recent years, but, at the same time, counterfeiters continue to hone their craft to counter these methods. This can perpetuate the potential for parts to escape process flows that only include techniques designed

to reveal disguises. Without applying tests to reveal damage associated with counterfeiting operations, escapes may occur that can affect performance in the end use application. (back)

C10: 'MIL-Spec' Versus Industry Standard Test Methods

Concerns are voiced on occasion about the use of 'MIL-Spec' test methods for counterfeit detection. These concerns tend to surround commercial and industrial grade components where conditions for 'environmental tests' may exceed the use conditions specified by the device manufacturer. Tests such as thermal cycle testing, fine and gross leak testing, and burn-in (including electrical testing as acceptance criteria) are frequently associated with military standard test methods for 'MIL-Spec' parts. These tests are also defined by industry standards developed by semiconductor physics and packaging reliability subject matter experts to apply to commercial parts in conjunction with ongoing failure-mechanism-driven reliability monitoring. Elevated stresses are used to produce failure mechanisms observed under use conditions, but in a shorter time period. These elevated stresses can include exposure to higher and lower temperatures and higher moisture than would be associated with normal use conditions.

Research conducted by SEMATECH paved the way to reliability evaluation methods used today by the semiconductor manufacturing industry …

- *"Use Condition Based Reliability Evaluation of New Semiconductor Technologies,"*[32] *SEMATECH Tech Transfer Document 99083810A-XFR, August 20, 1999*
- *"Comparing the Effectiveness of Stress-based Reliability Qualification Stress Conditions,"*[33] *SEMATECH Tech Transfer Document 04034510A-TR, April 12, 2004*
- *JEDEC Publication JEP122G, "Failure Mechanisms and Models for Semiconductor Devices"*[34]

Industry standards defining tests currently used by the semiconductor industry include the 'JEDEC Standards'[35], such as …

- *JESD22-A101 Steady State Temperature Humidity Bias Life Test*
- *JESD22-A104 Temperature Cycling*
- *JESD22-A108 Temperature, Bias, and Operating Life*
- *JESD22-A110 Highly Accelerated Temperature and Humidity Stress Test (HAST)* *(back)*

C11: Assembly And Equipment Level Tests

Do not assume that assembly and equipment level tests will detect counterfeit parts that may be contained within them. Determine the extent to which assembly and equipment level testing replicates part level tests designed to detect counterfeits.

When assessing field performance as the basis for the risk assessment of untraceable parts, verify the assemblies included in that assessment contain the same untraceable parts, and determine the extent to which field use replicates part level tests designed to detect counterfeits. (back)

---

[32] http://www.sematech.org/docubase/abstracts/99083810A-XFR.htm
[33] http://www.sematech.org/docubase/abstracts/04034510A-TR.htm
[34] http://www.jedec.org/standards-documents
[35] http://www.jedec.org/standards-documents

Appendix D. Case Studies

This appendix provides two case studies that provide specific examples of the actions taken to prevent counterfeit parts from being installed in government products.

CASE STUDY #1 – DUE DILLIGENCE FOR GMF AND CFM

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. 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:

- When purchases from sources of supply other than the original component manufacturer and its authorized distribution chain are necessary, due diligence should be performed to avoid counterfeits.
- When counterfeits are discovered, steps should be taken to avoid reintroducing counterfeits into the supply chain.
- U.S. 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 OCM 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 to notify government and industry of this finding. NAWCAD notified 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.

Considerations for Government Furnished Material (GFM) and Customer Furnished Material (CFM)

Users should not assume that GFM (including product sources through DLA) or CFM was acquired from authorized suppliers. In the case where GFM or CFM was acquired from authorized suppliers, do not assume that sufficient due diligence was performed to ensure the products furnished by customers of the government sources are not counterfeit products.

CASE STUDY #2 – "IF YOU ARE GOING TO RELY ON PAPER, AT LEAST DO MORE THAN JUST RELY ON THE DOCUMENT ITSELF."

The "China Law Blog" posting on "China Business Scams and How to Avoid Them"[36] includes an important lesson about depending on documentation to establish confidence in business practices and products. …

> *"There is probably no document that has not been faked thousands of times in China. I have seen fake bills of lading, fake bank statements, fake contracts, fake purchase orders, fake company registrations, fake IP registrations, even fake lawyers. If you are going to rely on paper, at least do more than just rely on the document itself. At minimum, check with the company or the governmental body that purportedly issued it."*

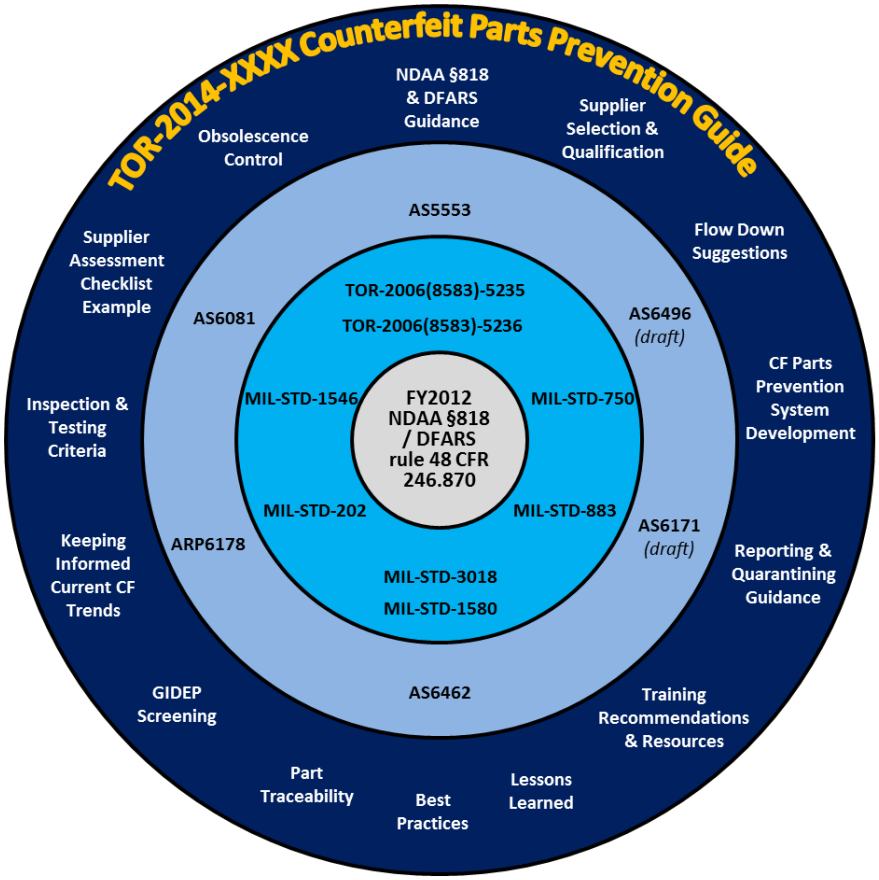
Those involved in counterfeit avoidance and detection activity can learn from this as it relates to certificates of compliance (CofC), test reports, and other documentation provided as evidence that a product is authentic. Applicable industry documents such as SAE TB-0003, TOR-2006(8583)-5235, TOR-2006(8583)-5236, and SAE International Standard AS5553 provide valuable insight in this area.

Though this specific article is presented in the context of the practical aspects of Chinese law and how it impacts business in China, the problem of bogus documentation is not unique to China.

[36] http://www.chinalawblog.com/2012/09/china-business.html

Appendix E. How This Guide Fits in the Total Picture

Appendix E is a pictorial representation of how the Counterfeit Parts Prevention Guide aligns with Federal Law and DFARS, military requirements, and industry standards. Information from each of these sources have been incorporated to provide a comprehensive guide.



AS5553, *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition*
- Generic requirements to flow down throughout the supply chain to procure / integrate electronic parts
- Risk-based mitigation depending on desired performance or reliability of the equipment/hardware

AS6081, *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition Distributors*
- Practices & requirements for distributors purchasing & selling EEE parts on the open market
- Does not apply to those that purchase and sell parts directly from OCMs or their authorized distributors

AS6462, *AS5553 Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition Verification Criteria*
- Standardizes assessment criteria to certify to AS5553 requirements

ARP6178, *Counterfeit Electronic Parts: Tool for Risk Assessment of Distributors*
- Survey tool for evaluating a distributor's processes
- Generates score of distributor's capability/effectiveness

AS6496 (draft), *Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Authorized/Franchised Distribution*
- Identifies requirements for mitigating counterfeit products in the authorized distribution supply chain

AS6171 (draft), *Test Methods Standard: Counterfeit Electronic Parts*
- Standardizes methods to detect suspect counterfeit electronic parts
- Ensure consistency of supply-chain test techniques and requirements

TOR-2014-XXXX, Counterfeit Parts Prevention Guide
Provides a comprehensive treatment of counterfeit protection systems, supplier qualification, part traceability, inspection and testing, reporting and quarantining, requirements flow down, and training that supplements government and industry standards to support space application needs and provides lessons learned and best practices from government and industry SMEs.

Appendix F. Counterfeit Prevention, Detection and Avoidance Standards Applicability Analysis for Hardware Products

Appendix F is a matrix of various publications associated with counterfeit parts prevention. This includes military specifications, ISO, SAE International (e.g., AS5553, AS6081), TechAmerica, FAA, Semiconductor Equipment and Materials International (SEMI), and others. The matrix shows which standards have been adopted by the DOD, their applicability to different users (i.e., OCMs, OEMs, System Integrators, and Component Distributors) and whether the standard addresses elements such as product traceability, risk mitigation, procurement practices, verification/detection, containment/disposition, reporting, and obsolescence management.

Standard	Scope	DoD Adopted	USER				Product Traceability	Risk Mitigation	Procurement Practices	Verification / Detection	Containment / Disposition	Reporting	Obsolescence Management	Comments
			SI	OEM	CD	OCM								
Technical Operating Reports (TORs) / Military Specifications...														
TOR-2006(8583)-5235, Parts, Materials, and Processes Control Program for Space and Launch Vehicles	Parts, Materials, Processes Control Program		x	x	x	x	x	x	x	x				
TOR-2006(8583)-5236, Technical Requirements for Electronic Parts, Materials, and Processes Used in Space and Launch Vehicles	Parts, Materials, Processes Selection and Use		x	x	x	x	x		x					Does not cover counterfeit prevention, detection and avoidance elements.
MIL-STD-202, Test Method Standard Electronic and Electrical Component Parts	Uniform Test Methods		x	x		x		x		x				Does not cover counterfeit prevention, detection and avoidance elements.
MIL-STD-750, Test Methods for Semiconductor Devices	Uniform Test Methods		x	x		x		x		x				Does not cover counterfeit prevention, detection and avoidance elements.
MIL-STD-883, Test Method Standard Microcircuits	Uniform Test Methods		x	x		x		x		x				Does not cover counterfeit prevention, detection and avoidance elements.
MIL-STD-1546, Parts, Materials, and Processes Control Program for Space and Launch Vehicles	Parts, Materials, Processes Selection and Use		x	x	x	x	x	x	x	x				
MIL-STD-3018, Parts Management	Parts Management Program (PMP)		x	x		x	x	x	x	x	x	x	x	
MIL-STD-1580, Destructive Physical Analysis for Electronic, Electromagnetic, and Electromechanical Parts	Electronic Parts DPA Requirements		x	x		x		x		x				Does not cover counterfeit prevention, dection and avoidance elements.
International Organization for Standardization (ISO) ...														
ISO 9001 Quality Management Systems - Requirements	Parts, Materials, Assemblies and Equipment	17-Apr-01	x	x	x	x								Does not cover counterfeit prevention, detection and avoidance elements
SAE International ...														
SAE AS9100 Quality Systems – Aerospace – Model for Quality Assurance in Design, Development, Production, Installation and Servicing	Parts, Materials, Assemblies and Equipment	1-Mar-02	x	x	x	x								Does not cover counterfeit prevention, detection and avoidance elements
SAE AS9120 Quality Management Systems – Aerospace Requirements for Stockist Distributors	Parts, Materials and Assemblies				x				x					General requirement to "prevent the purchase of counterfeit/suspect unapproved products." No criteria.
SAE AS9003 Inspection and Test Quality System	Electronic Components		x	x	x	x								Does not cover counterfeit prevention, detection and avoidance elements
SAE AS5553 Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition	Electronic Components	31-Aug-09	x	x			x	x	x	x	x	x	x	Released April 2009 Revised January 2013 Comprehensive coverage for all elements

Standard	Scope	DoD Adopted	USER				Product Traceability	Risk Mitigation	Procurement Practices	Verification / Detection	Containment / Disposition	Reporting	Obsolescence Management	Comments
			SI	OEM	CD	OCM								
SAE AS6174 Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel	Parts and materials	17-Jun-13	X	X			X	X	X	X	X	X		Released May 2012
SAE AS6081 Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors	Electronic Components	10-Jun-13			X		X		X	X	X	X		Released November 2012
ARP6178 Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors	Electronic Components				X		X		X	X	X	X		Released December 2011
AS6462 AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria	Electronic Components		X	X			X	X	X	X	X	X	X	Released November 2012
Proposed AS6301 AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance,Detection,Mitigation,and Disposition – Distributors Verification Criteria	Electronic Components		X	X	X		X		X	X	X	X		Work In Progress
Proposed AS6171 Test Methods Standard; Counterfeit Electronic Parts	Electronic Components		X	X	X					X				Work In Progress
Proposed AS6496 Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Authorized/Franchised Distribution	Electronic Components				X		X		X					Work In Progress
Proposed AIR6273 Terms and Definitions - Fraudulent/Counterfeit Electronic Parts	Electronic Components		X	X	X	X								Work In Progress
TechAmerica ...														
TechAmerica-TB-0003 Counterfeit Parts & Materials Risk Mitigation	Parts and materials		X	X			X	X	X	X	X	X		Released February 2009. High level guidance
EIA-4899 Standard for Preparing an Electronic Components Management Plan	Electronic Components		X	X									X	
EIA-933 Standard for Preparing a COTS Assembly Management Plan	Assemblies		X	X					X	X			X	Rev A requires a "Counterfeit Electronic Parts Control Plan" for flight critical assemblies
TechAmerica/ANSI STD-0016 Standard for Preparing a DMSMS Management Plan	Parts, Materials and Assemblies												X	Replaces EIA-GEB1
Federal Aviation Administration (FAA) ...														
FAA AC 00-56 Voluntary Industry Distributor Accreditation Program	Parts, Materials and Assemblies				X		X							Does not cover counterfeit prevention, detection and avoidance elements other than 'Product Traceabity'
JEDEC ...														
JESD31 General Requirements for Distributors of Commercial and Military Semiconductor Devices	Semiconductor Components	7-Sep-11			X		X							Traceability and C of C requirements for military semiconductor devices only.
Semiconductor Equipment and Materials International (SEMI) ...														
SEMI T20-0710 Specification for Authentication of Semiconductors and Related Products	Semiconductor Components					X	X							Defines a mechanism authenticate a product within the supply chain.
SEMI T20.1-1109 Specification for Object Labeling to Authenticate Semiconductors and Related Products In An Open Market	Semiconductor Components					X	X							Subordiate to SEMI T20-0710
SEMI T20.2-1109 Guide for Qualifications of Authentication Service Bodies for Detecting and Preventing Counterfeiting Of Semiconductors and Related Products	Semiconductor Components					X	X							Subordiate to SEMI T20-0710
Electronic Components, Assemblies and Materials Association (ECA) ...														
EIA/ECA-CB21 Counterfeit Passive Components	Passive Components		X	X							X	X		High level guidance

Standard	Scope	DoD Adopted	USER				Product Traceability	Risk Mitigation	Procurement Practices	Verification / Detection	Containment / Disposition	Reporting	Obsolescence Management	Comments
			SI	OEM	CD	OCM								
International Electrotechnical Commission (IEC) ...														
IEC/TS 62668-1 Process management for avionics - Counterfeit prevention - Part 1: Avoiding the use of counterfeit, fraudulent and recycled electronic components	Electronic Components		X	X	X	X	X	X	X	X	X	X		Released May 2012. High level guidance refering to other standards for implementation.
Proposed IEC/TS 62668-2 Process management for avionics - Counterfeit prevention - Part 2 (purchasing components outside of franchised distribution networks)	Electronic Components		X	X			X	X	X	X				Work In Progress. Per 4.12.13.2, GIFAS/5052/2008 to be adopted and modified to be published as IEC/TS 62668-2
Groupement des Industries Françaises Aéronautiques et Spatiales (GIFAS) ...														
GIFAS/5052/2008 Guide for managing electonic component sourcing through non-franchised distributors. Preventing fraud and counterfeiting.	Electronic Components		X	X			X	X	X	X				Released October 2008. High level guidance
Independent Distributors of Electronics Association (IDEA) ...														
IDEA-STD-1010 Acceptability of Electronic Components Distributed in the Open Market	Electronic Components				X					X				Includes inspection techniques for counterfeit detection.
Components Technology Institute, Inc ...														
CCAP-101 Counterfeit Components Avoidance Program, Certification For	Electronic Components				X		X		X	X				

LEGEND:

User (For use by):

- System Integrators (SI)
- Original Equipment Manufacturers (OEM)
- Component Distributors (CD)
- Original Component Manufacturers (OCM)

Counterfeit Prevention, Detection and Avoidance Elements:

- *Product Traceability:* methods to retain traceability of products from the original manufacturer to the end user.
- *Risk Mitigation:* approaches to assess and mitigate end use appication risks of procuring parts from riskier sources.
- *Procurement Practices:* procurement practices developed specifically to prevent the acquisition of counterfeit parts
- *Verification / Detection:* methods applied specifically to detect counterfeits
- *Containment / Disposition:* containment and disposition guidance for use when counterfeits are discovered
- *Reporting:* reporting guidance so that both industry and US Government organizations can determine whether or not they are similarly affected
- *Component Obsolescence Management:* includes guidance to address component obsolescence and, therefore, reduce the likelihood of having to acquire parts through riskier suppliers

Appendix G. Counterfeit Parts Process Audit Checklist Example

Appendix G provides an example of a checklist that could be used to assess suppliers on their capabilities of detecting and avoiding the inadvertent introduction of counterfeit electronic parts in the parts or assemblies they provide. The checklist may be tailored to ensure the most appropriate items are applied during a supplier assessment. Note that this checklist targets primarily microcircuits and discrete semiconductor products.

Supplier Audited:_____

Audit Date:_____

Auditor(s):_____

Reviewed by:

_____
Name
Title
Date

Approved by:

_____
Name
Title
Date

Prepared by:

_____
Name
Title
Date

_____
Name
Title
Date

Counterfeit Parts Audit Checklist (Example)

#	Question	Method of Verification Guidance	Results Accept/ Concern	Remarks Audit Notes
1	**General Information**			
1.1	Is the distributor being audited as franchise or independent?			
1.2	Is the distributor affiliated with any other distributors? What type of business relationship exists between the distributor and its affiliates?	Request to see evidence of transactions with affiliate distributors. Is the affiliated distributor a common source for hard to find parts? Verify parts' traceability documents.		
1.3	Is the distributor aware and hold a copy of Counterfeit Parts standard SAE International AS5553? Have any of those requirements being implemented within the facility?	Verify if the distributor holds a copy of SAE International AS5553. If so, request to see evidence of implementation of parts control plan per the standard.		
1.4	Have any customers flowed down any requirements listed in SAE International AS5553?	If yes, review a sample of customer purchase orders to verify if SAE International AS5553 shows as a requirement.		
1.5	Is the Distributor certified or compliant to SAE International AS6081?	Request evidence of distributor holding certification to SAE International AS6081.		
1.6	Do you currently sell product to DoD/NASA prime contractors, or to independent distributors who supply DoD/NASA prime contractors, or any other DoD/NASA organization?	If so, review sales receipts to DoD/NASA primes (e.g., Boeing, Lockheed Martin, Northrop, ATK…) review part traceability documents and assess whether it was purchased from a legitimate source.		
2	**Procurement**			
2.1	Do you purchase product from other distributors outside of the U.S., and who do you purchase from.	Review approved supplier list and identify foreign suppliers. Review several purchase orders to those foreign suppliers and question their legitimacy.		

Counterfeit Parts Audit Checklist (Example)

#	Question	Method of Verification Guidance	Results Accept/ Concern	Remarks Audit Notes
2.2	Does the distributor have an Approved Supplier List (ASL) and is it being maintained?	Request copy of ASL and assess several suppliers on the list, are there purchase orders to approved suppliers. Seek evidence on how the ASL is maintained.		
2.3	What is the process for approving and removing suppliers in the ASL system?	Review the supplier approval procedure and verify method for approving or removing suppliers from the ASL. If approved by auditing the supplier, verify audit results on several suppliers. Also, assess if a low rating causes removal of a supplier. If so, review causes of low supplier rating.		
2.4	How do you rate your suppliers, and what criteria do you use?	Verify procedure outlining criteria for rating a supplier and whether it is adequate. Ensure suppliers are rated on their ability to supply authentic product.		
2.5	How does the distributor ensure suppliers are providing authentic product? If not, how is it avoided?	Verify procurement documentation on several orders to ensure authentic product is being procured. ***Note:*** ***Agreed upon requirements must be verifiable at receiving inspection and parts testing.***		
2.6	Given multiple sources available from your ASL, would you buy product from a supplier with lower quality rating. If so, how do you mitigate potential risks of receiving a counterfeit / sub-standard part?	From the ASL, select several suppliers with low rating and verify if parts have been purchased lately. Assess whether appropriate justification was used for using a low rating supplier.		
2.7	What documentation (CoC, photos, etc…) is required from your suppliers prior to purchase of product.	Select several types of components and verify documentation on product received. Ensure documents follow a trail to authenticity of the component including photos.		

Counterfeit Parts Audit Checklist (Example)

#	Question	Method of Verification Guidance	Results Accept/ Concern	Remarks Audit Notes
2.8	Does the distributor have strict "Terms and Conditions" document for buying and selling?	If available, review the "Terms and Conditions" document. Determine if adequacy on strict sub-tier supplier responsibility to provide authentic/traceable parts.		
2.9	Does the distributor have a robust process to screen new suppliers prior to doing business with them?	Verify the process for screening new suppliers. Is there evidence of assessing new supplier capabilities and clear traceability of parts?		
2.10	Does the distributor pursue authorized sources first? How is this ensured?	Assess whether their part locator process shows the steps taken in locating authentic parts from authorized sources first.		
2.11	Are there other risk mitigating measures used by the supplier to ensure buying legitimate/authentic electronic components?	Review buying process to ensure risk mitigating steps are taken to ensure authentic parts are purchased.		
2.12	When buying components from an unauthorized supplier, what type of risk mitigation action is taken?	Review several procurement documents to verify whether special risk measures are employed when procuring from unauthorized suppliers.		
2.13	How is it ensured that product from an authorized supplier is not mixed with other product?	Assess three key areas where product may be mixed such as receiving inspection, component testing, and storage areas.		
2.14	Is the distributor certified to: 1. ISO 9001 2. AS9120 3. ANSI/ESD S20.20 Under which Certification Bodies?	If distributor claims to be certified, request evidence of certification. Take a copy of certificates.		

Counterfeit Parts Audit Checklist (Example)

#	Question	Method of Verification Guidance	Results Accept/ Concern	Remarks Audit Notes
2.15	Does the distributor hold any other industry known certifications?	Ask if other certification exists. Take copies of certificates.		
2.16	How is it ensured that customer special requirements are met (e.g., date code, RoHS, vendor section).	Review a few customer purchase orders to assess whether special requirements have been imposed by customers. Verify evidence that those requirements have been carried out.		
3	**Parts Inspection, Verification, and Handling.**			
3.1	What traceability or authenticity records do you require with incoming shipments? Is this requirement ever waived?	Verify if their procedure requires traceability or authenticity of parts. Is it also evident that this requirement is included in purchase orders and subsequently verified in receiving inspection or other inspection areas?		
3.2	What type of traceability or authenticity records do you provide with shipped product? Is this provision ever waived?	Verify whether the distributor provides authenticity records with shipments. Review several orders shipped seeking evidence of authenticity records.		

Counterfeit Parts Audit Checklist (Example)

#	**Question**	**Method of Verification** Guidance	**Results** Accept/ Concern	**Remarks** Audit Notes
3.3	What type of in-house test and/or inspection capabilities does the distributor have? Note: Circle in-house capabilities from the list provided.	Verify which of the following are performed: Documentation Check Physical Dimensions Visual Inspection (Texture and Characteristics) Lead inspection Marking permanency Solderability Test Decapsulation and Die Analysis X-Ray Analysis Scanning Acoustic Microscopy X-Ray Fluorescence Leak Test Basic Electrical Test (e.g., pin continuity, curve trace, LCR) Burn-In Test Functional Electrical Test, 25C Functional Electrical Test, Full Temperature Range. Destructive Physical Analysis (DPA)		

Counterfeit Parts Audit Checklist (Example)

#	**Question**	**Method of Verification** Guidance	**Results** Accept/ Concern	**Remarks** Audit Notes
3.4	Does the distributor outsource any test inspections to external test or inspection labs? Note: Circle outsourced inspections from the list provided.	Verify which of the following are performed: Documentation check (P/N, Qty, CoC) Physical dimensions Lead Inspection Marking permanency Solderability Test Decapsulation and Die Analysis X-Ray Analysis Scanning Acoustic Microscopy X-Ray Fluorescence Leak Test Basic Electrical Test (e.g., pin continuity, curve trace, LCR) Burn-In Test Functional Electrical Test, 25C Functional Electrical Test, Full Temperature Range. Destructive Physical Analysis (DPA)		
3.5	Are there any other inspection/test capabilities to verify authenticity of parts either in-house or out-sourced?	Ask if the distributor has other capabilities not listed in sections 3.3 and 3.4 above. If any, ask how those tests ensure part authenticity.		
3.6	Are all handling/storage areas compliant or certified to ANSI/ESD S20.20?	Verify that all component handling areas and personnel are compliant to ANSI/ESD S20.20 standard meeting guidelines set in tables 1, 2, and 3.		
3.7	How are external test labs assessed, approved and monitored for quality?	Review criteria used for assessing external labs. Seek evidence on how labs are approved. Are on-site assessments performed? How are these labs and approved status maintained?		

Counterfeit Parts Audit Checklist (Example)

#	Question	Method of Verification Guidance	Results Accept/ Concern	Remarks Audit Notes
3.8	Does the distributor have a robust process for inspecting product capable of detecting counterfeit and/or sub-standard parts?	Review the distributor's inspection criteria. Ensure it follows a best practice approach to inspecting product for detecting counterfeit/substandard components.		
3.9	At what magnification level are inspections done to? Does the distributor have magnified digital photo capability?	Review several inspection records to verify magnification level used while inspecting product. Do the records indicate evidence of digital photo capability? Ask if distributor has this capability.		
3.10	Does the distributor have visual inspection capabilities which include magnification?	Select a sample of microscopes or other visual inspection equipment used and verify if it is capable of reaching magnification levels required.		
3.11	What other visual inspection techniques does the distributor use?	Assess the inspection area to verify if additional visual inspections are performed.		
3.12	How is physical dimensional inspection performed, is the distributor using a caliper, micrometer, or optical comparator?	Assess the distributor's inspection area and note the type of equipment utilized to perform physical dimensioning of parts.		
3.13	Does the inspection process differ when inspecting parts from authorized versus unauthorized suppliers?	Review inspection criteria and several records of completed inspections on parts procured from authorized and unauthorized suppliers and compare.		
3.14	Does the distributor perform Marking Permanency Test (mineral spirits and alcohol) in-house? Is this performed on all parts?	Verify several completed test records to ensure they include the marking permanency test as performed. If not performed on all parts, question why.		

Counterfeit Parts Audit Checklist (Example)

#	Question	Method of Verification Guidance	Results Accept/ Concern	Remarks Audit Notes
3.15	Are other chemicals used in-house to check marking or surface finishes?	Review inspection procedure and assess whether other marking or surface finish checks are being performed.		
3.16	How are third-party test facilities assessed for suitability and authenticity testing?	Request to see records of on-site audits performed at third-party facilities. Do those audits ensure all capabilities are assessed?		
3.17	Is the original component manufacturer's data sheet being reviewed?	Select several receiving inspection documents of OCM parts procured and verify that data sheets are also reviewed as part of the inspection criteria.		
3.18	Of the inspections/tests described in Section 3.3 above, which are performed as standard practice?	Request the inspection criteria and assess which tests are performed on all parts. Use the list in section 3.3 and 3.4 to mark which tests are performed as standard.		
3.19	Are there any specific inspection/requirements procedures followed for NASA/U.S. Defense/Aerospace customers?	Verify test records on several types of components sold to NASA/U.S. Defense/Aerospace customers and compare to other components tested for industry customers.		
3.20	Have you ever been notified by a customer that you provided counterfeit/sub-standard suspect product? How was this issue addressed?	If yes, review customer communication records as evidence of notification that counterfeit parts were reported. Seek evidence on how this was handled.		
3.21	Is the distributor's storage and inspection areas temperature and humidity controlled, and to what levels?	Ask if storage areas are kept under temperature and humidity controlled environment, and ask per what requirement.		

Counterfeit Parts Audit Checklist (Example)

#	Question	Method of Verification Guidance	Results Accept/ Concern	Remarks Audit Notes
3.22	Does the distributor maintain a photo library of all parts procured, stocked, and shipped? Is the library used as reference to verify new part authenticity?	If so, review the photo collection and verify that it is being utilized as reference to identify authenticity of recent purchased parts.		
3.23	What type of inspection records do you maintain, and are they made available to customers.	Select a sample of records on inspected components and verify they are maintained. Ask if these are made available to customers.		
4	**Training**			
4.1	Does the distributor have a well-documented training plan in place?	Seek evidence that a documented process exists containing the inspection training plan at minimum.		
4.2	Are all inspectors performing inspections certified?	If yes, verify inspectors' qualifications and certifications training records. Note: is there other ways to ensure proper training for inspectors.		
4.3	How many component/QC inspectors do you have, and are they certified to an appropriate standard?	Request to see the list of certified inspectors. Verify several inspectors' names and ensure they are certified to an appropriate standard. Note if inspectors hold other inspection certifications.		
5	**Nonconforming Material**			
5.1	Does the distributor have a counterfeit parts control plan as required by SAE International AS5553?	Ask if the distributor has a counterfeit parts control plan whether it has been flowed down as a customer requirement or not.		

Counterfeit Parts Audit Checklist (Example)

#	Question	Method of Verification Guidance	Results Accept/ Concern	Remarks Audit Notes
5.2	Is there a process in place to disposition suspect counterfeit product? ***Note: DFARS 252.246-7007(c)(6) specifies that suspect counterfeit and counterfeit electronic parts are <u>NOT</u> returned to the supplier until determined to be authentic.***	Verify if the distributor has a well-documented process to disposition suspect counterfeit product and assess its adequacy.		
5.3	Does the distributor have a process to disposition confirmed counterfeit product?	Review documentation delineating the process for disposition of confirmed counterfeit product. Verify its adequacy and whether product is quarantined and permanently disposed of.		
5.4	How does the distributor scrap product?	Seek evidence of procedure followed to destroy nonconforming product.		
6	**Corrective Action**			
6.1	Is there a corrective action program, and under what circumstances is it required to initiate a corrective action request?	Verify that the distributor has a documented process for corrective action. Assess whether it includes the three steps: remedial, corrective, and preventive action including root cause analysis.		
6.2	Under what circumstances are internal corrective actions initiated?	Verify the effectiveness of corrective action taken. Review several closed corrective action files. Ensure it includes all the appropriate steps exhibiting effective implementation.		
6.3	Has the distributor ever shipped counterfeit product? And how did the distributor respond with respect to corrective/preventive actions?	Review several customer communication records and verify whether it has been communicated that customer has received counterfeit product. Verify records and that appropriate corrective action was taken.		
7	**Document Control and Record Retention**			

Counterfeit Parts Audit Checklist (Example)

#	Question	Method of Verification Guidance	Results Accept/ Concern	Remarks Audit Notes
7.1	Does the document control system require management review and approval?	Review documentation that delineates an effective document control system. Does the process include management review and approval?		
7.2	Are all documents with latest revisions available at point of use?	Select several work stations and verify that latest procedures and work instructions are readily available to personnel performing the work.		
7.3	What is the retention period for all quality, purchasing, and part traceability and authentication records?	Review record retention procedure and several closed quality and procurement files. Verify that records are being retained per their procedure. Verify required length for record retention dates are being met.		
8	**Reporting of suspect parts**			
8.1	Does the distributor report any suspect counterfeit/sub-standard parts to GIDEP? If so, how often? ***Note: DFARS 252.246-7007(c)(6) requires reporting suspect counterfeit and counterfeit parts to GIDEP.***	Review records and reports submitted during the last 12 months.		
8.2	Are confirmed counterfeit/suspect parts reported to any investigative agencies	Request to see any documentation indicating that counterfeit product has been reported to authorities shortly after being discovered. If no records are available, verify if there is a documented process in place at minimum.		

Counterfeit Parts Audit Checklist (Example)

#	Question	Method of Verification Guidance	Results Accept/ Concern	Remarks Audit Notes
8.3	What additional steps are taken to alert peers and/or customers on counterfeit/substandard parts?	Review records of supplier, affiliates and customer communication to verify how peers are made aware of discovered counterfeit/substandard parts. ***Note: This type of awareness allows for other organizations become vigilant on specific type of suspect parts to avoid shipping bad parts inadvertently***.		
9	**Liability and Disposition**			
9.1	What guarantees or warranties are offered for product sold?	Review several records of product shipped. Verify the type of warrantees or guarantees offered (implicit or explicit)		
9.2	Do you provide a standard product warranty period with all shipments? What is that period?	Review records of sold product and verify whether a warranty period is provided.		
9.3	What is the distributor's policy for accepting return of suspect counterfeit/substandard product from a customer?	Ask if the distributor has a policy for accepting counterfeit/substandard product. Verify the process for handling returned product as in 3.20 above.		
9.4	Does the distributor buy and/or sell product under escrow agreements?	Verify whether the distributor buys/sells product under escrow arrangement. Assess if appropriate controls are in place to ensure authenticity of product.		
9.5	Is used or refurbished product clearly identified before selling it to customers?	Assess the inspection and marking areas to verify that product is appropriately identified to confirm product purchased.		

Counterfeit Parts Audit Checklist (Example)

#	**Question**	**Method of Verification** Guidance	**Results** Accept/ Concern	**Remarks** Audit Notes
9.6	Does the distributor maintain "Preferred" status with any NASA/U.S. Defense/Aerospace customers? Provide list of customers.	Verify if the distributor maintains a "preferred" list of customers. If so, are any government agencies listed?		

RESULTS CODES :

M = MAJOR NONCONFORMANCE
N = MINOR NONCONFORMANCE
O = OBSERVATION
C = COMMENDATION
S = VERIFIED SATISFACTORY
N/A = NOT AUDITED

Appendix H. Checklist for Reporting Counterfeits

Appendix H provides a checklist of items to consider when reporting the discovery of counterfeit electronic parts to law enforcement agencies. This checklist does not take the place of contractual and regulatory reporting requirements. Companies should consult legal counsel for guidance regarding reporting outside of the company.

1. Contact Information

- ☐ Company/Agency Name:
- ☐ Address:
- ☐ Point of Contact:
- ☐ Work Phone:
- ☐ Mobile Phone:
- ☐ E-mail:
- ☐ Fax:

Note that an anonymous report may be submitted to law enforcement regarding a counterfeit good. However, doing so could limit or otherwise compromise authorities' efforts to conduct an investigation based on your information.

2. Description of Counterfeit Item

Describe the item that the company believes has a counterfeit trademark/service mark/certification mark. Include the name of the apparent manufacturer, part number, lot code, date code, country of origin, part markings, and other manufacturing information. Provide high-quality photographs of the item (front and back) and the counterfeit mark.

- ☐ Describe the counterfeit mark.
- ☐ Is the mark registered on the principal register of the U.S. Patent and Trademark Office?
  ___ YES ___NO

  If yes, provide the following:
  - Registration Date:
  - Registration Number:
- ☐ Has the counterfeit item been preserved, documenting the chain of custody?
  ___ YES ___NO
- ☐ Provide information about the supplier/seller of the item, including any relevant documents or records.
  - Supplier name:
  - Physical address:
  - Website:
  - Contact individual:
  - Phone number:
  - E-mail address:
  - Other identifiers:
- ☐ Provide information about the supply/purchase of the item, including any relevant documents or records.
  - Quantity purchased:
  - Unit price and total price:

- Item specifications, special terms and conditions, or quality or conformance requirements:
- Date and time of purchase:
- Method of payment:
- Describe communications with supplier (provide copies):
- Other information about supply/purchase:

- Provide information about the shipping/installation of the item, including any relevant documents or records.
  - Date and manner of shipment/delivery of item:
  - Other items included in shipment with item:
  - Date and time of installation (if any):
  - Date and time of repair (if any):
- If any other companies/individuals were involved in supplying/selling the counterfeit good, provide the same information requested above (if known) for each of those companies/individuals.
- What is the approximate retail value of the infringed good (i.e., the authentic good if purchased directly from the OEM/OCM or authorized distributor)?
- Describe how the counterfeit item was discovered including the date of discovery and details regarding any inspection, examination, analysis, evaluation, failure, or testing. Provide all inspection, examination, analysis, evaluation, failure, and testing reports.
- Describe the reasons it is believed the good is counterfeit, including whether the item is recycled or remarked, and any specific indicators of counterfeiting.
- Describe any reporting database consulted regarding the supplier or the item, and what was discovered.
- Have any goods from this supplier been received previously? Provide details regarding that supply/purchase.
- If goods were previously received from this supplier, were any of those later determined or suspected to be counterfeit? ___YES ___NO

  If yes, was the supplier placed on notice that a counterfeit good was received? Were any contractual actions taken against the supplier? Any administrative action? Any civil action? Was there a criminal referral? Please provide all relevant details. In addition, if the government took any legal action against the supplier, identify the name of the court or administrative body and case/complaint number; date of filing; names of attorneys; and status of case/complaint.
- Is the company aware of whether the supplier, in connection with counterfeit goods, has been the subject of an allegation of breach of contract or a previous civil, administrative, or criminal enforcement action not described above? If so, provide a general description of the matter as well as the name of the court or administrative body and case/complaint number (if known).
- If an internal investigation regarding the counterfeit good has been conducted, describe any evidence acquired not described above and submit, if possible, all investigative reports.
- Describe the company's estimated losses thus far from discovery of the counterfeit good.

3. Origin and Entry into the United States (If Applicable)

- ☐ Identify the country of origin of the counterfeit item.
- ☐ Identify the date, location, and mode of entry into the United States.
- ☐ Provide applicable shipping and customs information including the names of shippers or other entities/individuals involved in the shipping process as well as the Harmonized Tariff Schedule (HTS) designation for the shipment. More information about HTS designations may be found at: http://hts.usitc.gov.

4. Additional Information, Records, and Documents

- ☐ Provide any information concerning the suspected crime or violation of law not described above that might assist law enforcement.

AEROSPACE REPORT NO.
TOR-2014-02200

Counterfeit Parts Prevention Strategies Guide

Approved Electronically by:

Russell E. Averill, GENERAL MANAGER
SPACE BASED SURVEILLANCE DIVISION
SPACE PROGRAM OPERATIONS
SPACE SYSTEMS GROUP

Jacqueline M. Wyrwitzke, PRINC DIRECTOR
MISSION ASSURANCE SUBDIVISION
SYSTEMS ENGINEERING DIVISION
ENGINEERING & TECHNOLOGY GROUP

Jackie M. Webb-Larkin, SECURITY SPECIALIST III
GOVERNMENT SECURITY
SECURITY OPERATIONS
OPERATIONS & SUPPORT GROUP

Technical Peer Review Performed by:

Jacqueline M. Wyrwitzke, PRINC DIRECTOR
MISSION ASSURANCE SUBDIVISION
SYSTEMS ENGINEERING DIVISION
ENGINEERING & TECHNOLOGY GROUP

SK0671

External Distribution

REPORT TITLE		
Counterfeit Parts Prevention Strategies Guide		
REPORT NO.	PUBLICATION DATE	SECURITY CLASSIFICATION
TOR-2014-02200	June 24, 2014	UNCLASSIFIED

Charles Abernethy
charles.abernethy@aerojet.com
Aerojet

Scott Anderson
scott.anderson@seaker.com
Seaker

Ken Baier
ken.b.baier@lmco.com
Lockheed Martin

Carlo Abesamis
abesamis@jpl.nasa.gov
NASA

Aaron Apruzzese
aaron.apruzzese@atk.com
ATK

Dean Baker
bakerdea@nro.mil
NRO

Andrew Adams
andrew.c.adams@boeing.com
Boeing

Chic Arey
areyc@nro.mil
NRO

Mark Baldwin
Mark.L.Baldwin@raytheon.com
Raytheon

David Adcock
adcock.david@orbital.com
Orbital

Brent Armand
Armand.Brent@orbital.com
Orbital

Lisa Barboza
Lisa.Barboza@gd-ais.com
General Dynamics

Robert Adkisson
robert.w.adkisson@boeing.com
Boeing

Larry Arnett
arnett.larry@ssd.loral.com
Loral

Glenn Barney
glenn.barney@comdex-use.com
Comdev-USA

David Beckwith
beckwith@nro.mil
NRO

Christopher Brust
Christopher.Brust@dcma.mil
DCMA

Will Caven
caven.will@ssd.loral.com
Loral

Theresa Beech
tbeech@metispace.com
Metispace

Alexis Burkevics
Alexis.Burkevics@rocket.com
Rocket

Shawn Cheadle
shawn.cheadle@lmco.com
Lockheed Martin

Barry Birdsong
barry.birdsong@mda.mil
MDA

Thomas Burns
thomas.burns@noaa.gov
NOAA

Janica Cheney
janica.cheney@atk.com
ATK

Ruth Bishop
ruth.bishop@ngc.com
Northrop Grumman

Edward Bush
Edward.Bush@ngs.com
Northrop Grumman

Brian Class
class.brian@orbital.com
Orbital

Robert Bodemuller
rbodemuller@ball.com
Ball

Tim Cahill
tim.cahil@lmco.com
Lockheed Martin

Brad Clevenger
brad_clevenger@emcore.com
EMCORE

Silvia Bouchard
silver.bouchard@ngc.com
Northrop Grumman

Kevin Campbell
kevin.campbell@exelisinc.com
Exelis Inc

Jerald Cogen
Jerald.Cogen@FreqElec.com
FREQELEC

Wayne Brown
wayne.brown@ulalaunch.com
ULA Launch

Larry Capots
larry.capots@lmco.com
Lockheed Martin

Bernie Collins
bernie.f.collins@dni.gov
DNI

Jeff Conyers
jconyers@ball.com
Ball

Douglas Dawson
douglas.e.dawson@jpl.nasa.gov
NASA

David Eckhardt
david.g.eckhardt@baesystems.com
BAE Systems

Kevin Crackel
kevin.crackel@aerojet.com
Aerojet

Jaclyn Decker
decker.jaclun@orbital.com
Orbital

Robert Ellsworth
robert.h.ellsworth@boeing.com
Boeing

James Creiman
James.Creiman@ngc.com
Northrup Grumman

Larry DeFillipo
defillipo.aryy@orbital.com
Orbital

Matt Fahl
mfahl@harris.com
Harris Corporation

Stephen Cross
stephen.d.cross@ulalaunch.com
ULA Launch

Ken Dodson
ken.dodson@sslmda.com
SSL MDA

James Farrell
james.t.farrell@boeing.com
Boeing

Shawn Cullen
shawn.cullen@jdsu.com
JDSU

Tom Donehue
tom.donehue@atk.com
ATK

Tracy Fiedler
tracy.m.fiedler@raytheon.com
Raytheon

Louis D'Angelo
louis.a.d'angelo@lmco.com
Lockheed Martin

Mary D'Ordine
mdordine@ball.com
Ball

Brad Fields
fields.brad@orbital.com
Orbital

David Davis
David.Davis.3@us.af.mil
SMC

Susanne Dubois
susanne.dubois@ngc.com
Northrop Grumman

Sherri Fike
sfike@ball.com
Ball

Richard Fink
richard.fink@nro.mil
NRO

Matteo Genna
matteo.genna@sslmda.com
SSL

Joe Haman
jhaman@ball.com
Ball

Bruce Flanick
bruce.flanick@ngc.com
Northrop Grumman

Helen Gjerde
helen.gjerde@lmco.con
Lockheed Martin

Lilian Hanna
lilian.hanna@boeing.com
Boeing

Mike Floyd
Mike.Floyd@gdc4s.com
General Dynamics

Ricardo Gonzalez
ricardo.gonzalez@baesystems.com
BAE Systems

Harold Harder
harold.m.harder@boeing.com
Boeing

David Ford
david.ford@flextronics.com
Flextronics

Dale Gordon
dale.gordon@rocket.com
Rocket

Bob Harr
bob.harr@seaker.com
Seaker

Robert Frankievich
robert.h.frankievich@lmco.com
Lockheed Martin

Chuck Gray
Chuckg@fescorp.com
Fescorp

Frederick Hawthorne
frederick.d.hawthorne@lmco.com
Lockheed Martin

Bill Frazier
wfrazier@ball.com
Ball

Luigi Greco
luigi.greco@exelisinc.com
Exelis Inc

Ben Hoang
Hoang.Ben@orbital.com
Orbital

Jace Gardner
jgardner@ball.com
Ball

Gregory Hafner
Hafner.Gregory@orbital.com
Orbital

Rosemary Hobart
rosemary@hobartmachined.com
Hobart Machined

Richard Hodges
richard.e.hodges@jpl.nasa.gov
NASA

Amanda Johnson
johnson.amanda@orbital.com
Orbital

Mark King
markking@micropac.com
Micopac

Paul Hopkins
paul.c.hopkins@lmco.com
Lockheed Martin

Edward Jopson
edward.jopson@ngc.com
Northrop Grumman

Andrew King
andrew.m.king@boeing.com
Boeing

Kevin Horgan
kevin.horgan@nasa.gov
NASA

Jim Judd
judd.jim@orbital.com
orbital

Byron Knight
knightby@nro.mil
NRO

Eugene Jaramillo
eugenejaramillo@raytheon.com
Raytheon

Geoffrey Kaczynski
gkazynik@neaelectonics.com
NEA Electronics

Hans Koenigsmann
hans.koenigsmann@spacex.com
SpaceX

Dan Jarmel
dan.jarmel@ngc.com
Northrop Grumman

Mike Kahler
mkahler@ball.com
Ball

James Koory
james.koory@rocket.com
Rocket

Robert Jennings
rjennings@raytheon.com
Raytheon

Yehwan Kim
ykim@moog.com
Moog

Brian Kosinski
Kosinski.Brian@ssd.loral.com
SSL

Mike Jensen
mike.jensen@ulalaunch.com
ULA Launch

Jeff Kincaid
Jeffrey.Kincaid@pwr.utc.com
Power

John Kowalchik
john.j.kowalchik@lmco.com
Lockheed Martin

Rick Krause
rkrause@ball.com
Ball

Eric Lau
lau.eric@ssd.loral.com
SSL

Henry Livingston
henry.c.livingson@baesystems.com
BAE Systems

Steve Krein
steve.krein@atk.com
ATK

Marvin LeBlanc
Marvin.LeBlanc@noaa.gov
NOAA

Art Lofton
Art.Lofton@ngc.com
Northrop Grumman

Steve Kuritz
steve.kuritz@ngc.com
Northrop Grumman

Scott Lee
Scott.lee@ngc.com
Northrop Grumman

James Loman
james.loman@sslmda.com
SSL

Louise Ladow
louise.ladow@seaker.com
Seaker

Don LeRoy
dleroy@bardenbearings.com
Barden Bearings

Jim Loman
loman.james@ssd.loral.com
SSL

C J Land
cland@harris.com
Harris

Scot Lichty
scot.r.lichty@lmco.com
Lockheed Martin

Lester Lopez
llopez04@harris.com
Harris

Chris Larocca
clarocca@emcore.com
EMCORE

Sultan Ali Lilani
sultan.lilani@integra-tech.com
Integra - Tech

Frank Lucca
frank.l.lucca@1-3com.com
1-3 Com

Robert Lasky
lasky.robert@orbital.com
Orbital

Josh Lindley
joshua.lindley@mda.mil
MDA

Joan Lum
joan.l.lum@boeing.com
Boeing

Brian Mack
mack.brian@orbital.com
Orbital

Jeff Mendenhall
mendenhall@ll.mit.edu
MIT

Deanna Musil
deanna.musil@sslmda.com
SSL

Julio Malaga
malaga.julio@orbital.com
Orbital

Jo Merritt
jmerritt@avtec.com
AVTEC

Thomas Musselman
thomas.e.musselman@boeing.com
Boeing

Kevin Mallon
Kevin.P.Mallon@1-3com.com
1-3 Com

Charles Mills
charles.a.mills@lmco.com
Lockheed Martin

John Nelson
john.d.nelson@lmco.com
Lockheed Martin

Miroslav Maramica
miroslav@area51esq.com
Area 51

Edmond Mitchell
edmond.mitchell@jhuapl.edu
APL

Dave Novotney
dbnovotney@eba-d.com
EBA

John Mc Bride
Mcbride.John@orbital.com
Orbital

Dennis Mlynarski
dennis.mlynarski@lmco.com
Lockheed Martin

Ron Nowlin
ron.nowlin@eaglepicher.com
EaglePicher

Ian McDonald
ian.a.mcdonald@baesystems.com
BAE Systems

George Mock
gbm3@nyelubricants.com
NYE Lubricants

Mike Numberger
nurnberger@nrl.navy.mil
Navy

Kurt Meister
kurt.meister@honeywell.com
Honeywell

Nancy Murray
Nancy.murray@saftbatteries.com
Safety Batteries

Michael O'Brien
michael.obrien@exelisinc.com
Exelis Inc

Michael Ogneovski
michael.ognenovski@exelisinc.com
Exelis Inc

Paulette Megan
paulette.megan@orbital.com
Orbital

David Rea
david.a.rea@baesystems.com
BAE Systems

Debra Olejniczak
Debra.Olejniczak@ngc.com
Northrop Grumman

Mark Pazder
mpazder@moog.com
Moog

Forrest Reed
forrest.reed@eaglepicher.com
EaglePicher

Larry Ostendorf
Lostendorf@psemc.com
psemc

Steven Pereira
Steven.Pereira@jhuapl.edu
APL

Thomas Reinsel
thomas_j_reinsel@raytheon.com
Raytheon

Anthony Owens
anthony_owens@raytheon.com
Raytheon

Richard Pfisterer
Richard.Pfisterer@jhuapl.edu
APL

Bob Ricco
bob.ricco@ngc.com
Northrop Grumman

Joseph Packard
Joseph.packard@exelisinc.com
Exelis Inc

Angela Phillips
amphillips@raytheon.com
Raytheon

Mike Rice
mrice@rtlogic.com
RT Logic

Peter Pallin
peter.pallin@sslmda.com
SSL

Dave Pinkley
dpinkley@ball.com
Ball

Sally Richardson
richardson.sally@orbital.com
Orbital

Richard Patrican
Richard.A.Patrican@raytheon.com
Raytheon

Kay Rand
kay.rand@ngc.com
Northrop Grumman

Troy Rodriquez
troy_rodriquez@sierramicrowave.com
Sierra Microwave

Ralph Roe
ralph.r.roe@nasa.gov
NASA

Michael Sampson
michael.j.sampson@nasa.gov
NASA

Michael Settember
michael.a.settember@jpl.nasa.gov
NASA

Mike Roller
mike.roller@utas.utc.com
UTAS

Victor Sank
victor.j.sank@nasa.gov
NASA

Tom Sharpe
tsharpe@smtcorp.com
SMT Corp

John Rotondo
john.l.rotondo@boeing.com
Boeing

Don Sawyer
don.sawyer@avnet.com
AVNET

Jonathan Sheffield
jonathan.sheffield@sslmda.com
SSL

William Rozea
william.rozea@rocket.com
Rocket

Fred Schipp
frederick.schipp@navy.mil
MDA - Navy

Andrew Shroyer
ashroyer@ball.com
Ball

Dennis Rubien
dennis.rubien@ngc.com
Northrop Grumman

Jim Schultz
james.w.schultz@boeing.com
Boeing

Fredic Silverman
fsilverman@hstc.com
HSTC

Larry Rubin
Rubin.larry@ssd.loral.com
SSL

Gerald Schumann
gerald.d.schumann@nasa.gov
NASA

Rob Singh
rob.singh@sslmda.com
SSL

Lane Saechao
lane.saechao@rocket.com
Rocket

Annie Sennet
Annie.Sennet@saftbarries.com
Safety Batteries

Kevin Sink
kevin.sink@ttinc.com
TTINC

Melanie Sloane
melanie.sloane@lmco.com
Lockheed Martin

David Swanson
swanson.david@orbital.com
Orbital

Marvin VanderWeg
marvin.vanderwag@spacex.com
SpaceX

Jerry Sobetski
jerome.f.sobetski@lmco.com
Lockheed Martin

Mauricio Tapia
tapia.mauricio@orbital.com
Oribital

Gerrit VanOmmering
gerrit.vanommering@sslmda.com
SSL

LaKeisha Souter
lakeisha.souter@ngc.com
Northrop Grumman

Jeffrey Tate
jeffery_tate@raytheon.com
Raytheon

Michael Verzuh
mverzuh@ball.com
Ball

Jerry Spindler
Jerry.Spindler@exelisinc.com
Execlis Inc

Bill Toth
william.toth@ngc.com
Northrop Grumman

John Vilja
jussi.vilja@pwr.utc.com
Power UTC

Peter Stoltz
pstoltz@txcorp.com
TX Corp

Ghislain Turgeon
ghislain.turgeon@sslmda.com
SSL

Vinvent Stefan
vincent.stefan@orbital.com
Orbital

Thomas Stout
thomas.stout@ngc.com
Northrop Grumman

Deborah Valley
deborah.valley@ll.mit.edu
MIT

James Wade
james.w.wade@raytheon.com
Raytheon

George Styk
george.styk@exelisinc.com
Exelis Inc

Fred Van Milligen
fvanmilligen@jdsu.com
JDSU

John Walker
JohnF.Walker@sslmda.com
SSL

Brian Weir
weir_brian@bah.com
Booz Allen Hamilton

Larry Wray
wray.larry@ssd.loral.com
SSL

Arthur Weiss
arthur.weiss@pwr.utc.com
Power UTC

Mark Wroth
mark.wroth@ngc.com
Northrop Grumman

Craig Wesser
craig.wesser@ngc.com
Norhtrop Grumman

Jian Xu
jian.xu@aeroflex.com
Aeroflex

Dan White
dan.white@comdev-usa.com
Comdex-USA

George Young
gyoung@raytheon.com
Raytheon

Thomas Whitmeyer
tom.whitmeyer@nasa.gov
NASA

Charlie Whitmeyer
whitmeyer.charlie@orbtial.co
m
Orbital

Michael Woo
michael.woo@raytheon.com
Raytheon

APPROVED BY (AF OFFICE) Jim Roberts DATE June 30, 2014