COUNTERFEIT MATERIEL PROCESS GUIDEBOOK

Guidelines for Mitigating the Risk Of Counterfeit Materiel in the Supply Chain

Published by the Office of the Assistant Secretary of the Navy (Research, Development & Acquisition) Acquisition and Business Management

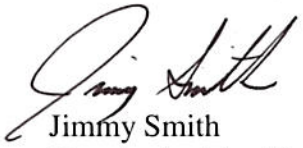
June 2017
NAVSO P-7000

This page intentionally left blank

Foreword

In recent years, manufacturers supplying products to the Department of Defense (DoD) have encountered a dramatic increase of counterfeit materiel in the supply chain. It affects all supply classes and poses a significant threat to readiness and reliability of our weapon systems, potentially resulting in the loss of materiel, mission or life. The United States Congress recognized these risks and enacted Section 818 of the National Defense Authorization Act for Fiscal Year 2012, "Detection and Avoidance of Counterfeit Electronic Parts," for implementation by DoD. In 2015, the Department of Navy (DON) published the Counterfeit Materiel Prevention Policy, SECNAVINST 4855.20, to provide implementing guidance to comply with the new requirements in public law. The policy requires all DON activities to implement a risk-based approach for identifying materiel that is at high risk of counterfeiting; mitigating use of that materiel; and reporting all instances of counterfeit and suspected counterfeit materiel.

The "Counterfeit Materiel Process Guidebook" is a follow-on effort to underscore the critical importance of counterfeit materiel prevention. The purpose of the guidebook is to equip DON activities with a practical tool for implementing a risk-based counterfeit materiel prevention program and provide implementing guidance to address the requirements delineated in the DON policy. Through a risk-based approach, DON activities will be able to apply engineering and sustainment principles for selection, assessment, and procurement of materiel; and mitigate the risk of counterfeit materiel plaguing our supply chain. The continual practical application of these principles minimize risks while ensuring that additional resources are not expended for items or applications that are of lower risk. This guidebook demonstrates our continuous focus on counterfeit materiel prevention and serves as a practical hands-on tool for all functional communities to combat the risks and impacts of counterfeit materiel on our weapon systems.



Jimmy Smith
Deputy Assistant Secretary of the Navy
(Expeditionary Programs & Logistics Management)

This page intentionally left blank

Table of Contents

This page intentionally left blank

Overview

This guidebook provides guidance and processes for implementing SECNAVINST 4855.20, Counterfeit Material Prevention, dated 22 April 2015. It is intended for use by all DON organizations to minimize the risk of counterfeit materiel entering the supply chain. This guidebook is broken down into seven Parts as follows:

- Part I, Assessing Counterfeit Materiel Risk
- Part II, Supplier Selection and Procurement
- Part III, Documentation
- Part IV, Contracting
- Part V, Detection
- Part VI, Containment, Disposition, and Reporting
- Part VII, Contractor Assessment

Introduction

Department of Navy (DON) policy requires DON activities to implement a risk-based approach to identify and prevent the introduction of materiel that is at high risk of counterfeiting. It also directs the DON to apply preventative measures, early detection processes, strengthened surveillance procedures, and accountable oversight commensurate with the end use application of the materiel in the system or its criticality, and to ensure all instances of counterfeit materiel or suspect counterfeit materiel are reported.

Counterfeit materiel poses a significant risk to the supply chain, potentially resulting in loss of materiel, mission, or life. Counterfeit materiel refers to items that are unauthorized copies or substitutes that have been identified, marked, or altered by a source other than the items' legally authorized supplier or have been misrepresented to be authorized items of the legally authorized supplier. Examples include but are not limited to:

- Used materiel sold as new
- Materiel represented as having specific capability (e.g., speed, power, temperature, capacity) beyond what the part was specified by the Original Manufacturer (OM)
- Material construction (e.g., anodization, composition) other than the materiel's advertised construction
- Materiel containing additional features or capabilities not intended by the OM (e.g., added malicious functions, modified firmware, etc.)

Counterfeit materiel is a serious threat to the safety and operational effectiveness of DON systems, as counterfeit materiel is often inferior to the authentic product. This inferiority manifests itself not only during initial system testing, but in reduced system life. Counterfeit materiel affects all supply classes, including but not limited to:

- Electronic parts such as integrated circuits, transistors, diodes, and resistors
- Mechanical parts such as valves, bearings, and fasteners
- Materials such as lubricants, adhesives, refrigerants, and batteries

It is reasonable to assume that if a materiel can be counterfeited, it will be. Additionally, the quality of counterfeiting has dramatically improved since the issue was first widely reported in 2007. Therefore, a continuously improving, diligent approach to purchasing, inspection, and test practices is critical if the adverse impact of counterfeit materiel is to be minimized for DON programs. In general, if the following rules are applied, the risks posed by counterfeit materiel will be minimized.

1. Purchase materiel from OMs and their authorized suppliers whenever possible. Materiel purchased from unauthorized suppliers is considerably more at risk of being counterfeit.
2. Practice proactive Diminishing Manufacturing Sources and Material Shortages (DMSMS) management. Obsolescence is a justifiable reason to purchase from an unauthorized supplier, if no other options exist. Proactive DMSMS management and technology refresh/insertion planning reduces the risk that obsolete parts must be procured from unauthorized suppliers.
3. Aggressively manage the supply chain to ensure unauthorized suppliers have been thoroughly vetted to reduce the risk of receiving counterfeit materiel.
4. Establish a risk-based set of inspections and tests proven to detect counterfeit materiel.
5. Establish a standardized process for reporting suspect counterfeit parts to all pertinent stakeholders, including Naval Criminal Investigative Service (NCIS), the Navy Assistant General Counsel Acquisition Integrity Office, the contracting officer, the pertinent chain of command (including security officer), and all users of the materiel. Never contact the supplier of the materiel. Initiate Product Quality Deficiency Reports (PQDRs) using Detailed Cause Code "5AS" for counterfeit and suspect counterfeit materiel.
6. Report counterfeit and suspect counterfeit materiel to the Government-Industry Data Exchange Program (GIDEP) within 60 days of suspicion the materiel is counterfeit.
7. Train all affected personnel (e.g., program management, purchasing, inspection, test, production, engineering, quality, and repair) in the prevention, detection, containment, reporting, and disposition of counterfeit materiel, to be in alignment with DON requirements to mitigate risk in the supply chain.
8. Contractually obligate contractors and their sub-contractors to implement counterfeit mitigation practices, including those described above.

Part I: Assessing Counterfeit Materiel Risk

Objective:

To identify the process for assessing the risk of incorporating counterfeit materiel into a system under design and during sustainment.

1.1 Introduction

During design and selection of materiel, the risk of counterfeit materiel needs to be assessed and mitigations examined. While this is a continual part of the risk management process and is initiated throughout the materiel selection process, the first formal assessment should take place as part of the Preliminary Design Review (PDR) and the following applicable Systems Engineering Technical Reviews (SETR). Assessments to determine the risk of counterfeiting must also be considered as part of the Engineering Change Proposal (ECP) process. The SETRs such as the PDR assessment criteria should include considerations for:

- Technology roadmap of the parts and material selected and the long term availability of the materiel
- Stability of the suppliers and location (region) of the suppliers
- Criticality of the materiel
- Criticality of the application
- Susceptibility to counterfeiting

The following provides factors for consideration when assessing counterfeit risk. While cost and schedule are key to the risk assessment process, this section focuses on technical risk.

1.2 Impact

Potential impact or consequences of materiel being counterfeit includes decreased functionality and reliability, unexpected behavior, decreased interoperability, and targeted malicious attack. The severity of the impact drives higher risk.

- **Criticality:** Materiel that is critical to mission success or personnel safety carries a higher potential impact if that materiel were to be counterfeit. Systems engineers and mission/operator representatives are responsible for identifying and documenting critical materiel throughout the acquisition life-cycle, in accordance with DODI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, and DODI 5000.02, Operation of the Defense Acquisition System, per the process documented in the Program Protection Plan (PPP). The end-to-end system must be considered, including items such as mission packages, government furnished components, and interdependent systems that may be outside a program manager's control.

  Appendix A defines the four types of critical materiel referenced in SECNAVINST 4855.20. Along with those four types (Critical Safety Items (CSI), Critical Application Items (CAI), Controlled Inventory Items (CII), and Information and Communications Technology (ICT) Components), SECNAVINST 4855.20 also requires critical materiel

to be defined by the responsible engineering support activity, if the materiel is considered to be at high risk for counterfeiting, and any materiel identified by the responsible engineering support activity prior to initial supportability analysis that has been documented by the responsible logistics organization.

- **Strategic Value:** Special precautions should be taken for materiel that would provide tactical or strategic value to any foe able to intentionally target the item with a malicious attack. Examples include materiel that stores or transmits valuable information, controls or activates critical items, or creates a vulnerability window by which other critical materiel within the system may be accessed (such as memory devices, programmable devices, and networking equipment). A targeted malicious attack is increasingly likely to take the form of embedded software or firmware, but can still manifest as compromised physical configuration or integrity.

  Manufacturing is increasingly being moved to foreign countries in order to take advantage of cheaper labor and manufacturing costs. Some of the locations may be considered adversarial, or at least non-friendly to DON systems. While critical materiel from these locations might not be highly susceptible to counterfeiting, the potential system impact of maliciously inserted software, firmware, or hardware means that these assemblies should be vigorously assessed to avoid or detect potential malicious work. Malicious intent is currently thought to primarily involve 1) reporting of system data to an unfriendly party, or 2) allowing an unfriendly party to command the system at a future date.

1.3 Likelihood

It should be assumed that all materiel may be counterfeited. However, there are several factors that make an item more likely to be a target of counterfeiters.

- **Obsolescence –** Obsolete materiel is no longer available from trustworthy suppliers such as the OM or an authorized supplier. If the materiel is still in demand, the selling price may increase significantly, enough to justify counterfeiting.
- **Difficult to Procure** – Some materiel may present procurement challenges such as special waivers, rare materials, environmental concerns, etc. Falsification of documentation may allow noncompliant materiel to be sold fraudulently.
- **Procurement Lead Time** – Counterfeiters can often provide very short lead times for materiel, making the materiel a more attractive option when schedule is critical.
- **Multiple Versions** – Materiel with multiple compatible versions available can be profitably misrepresented. An example might be a common bolt or washer that is available in several different plating or heat treatment versions, or an integrated circuit with commercial, industrial, and military temperature ranges available. In these cases, lower-quality or lesser parts can be sold for a higher price.
- **Item Type** – Certain categories of items are identified as counterfeit more often than others. A 2012 Defense Logistics Agency (DLA) assessment of counterfeit risk within DLA's supply chain covered sixty-nine Federal Supply Groups (FSGs) managed by DLA. Figure 1 represents the assessment of low (green), moderate (yellow), and high (indicated as red) counterfeiting risks across those FSGs. The five highest risk FSGs were:

- FSG 59 – Electrical and Electronic Equipment Components, such as: Integrated circuits; Transistors; Diodes; Connectors, and Electronic assemblies
- FSG 29 – Engine Accessories, such as: Filters; valves, and pumps
- FSG 47 – Pipe, Tubing, Hose and Fittings
- FSG 53 – Hardware and Abrasives, such as: Nuts; Bolts; Washers; Screws; Brackets; Seals; O-Rings; Lubricants, and Abrasives
- FSG 25 –Vehicular Equipment Components, such as Brakes and Springs

Figure 1: Assessment of Counterfeit Risk for DLA-Managed FSGs

Integrated circuits are currently the most commonly counterfeited item. Figure 2 and Figure 3 show the breakdown of integrated circuits by type for counterfeiting. The circular arrow on Figure 3 denotes the types of integrated circuits most attractive for malicious tampering.

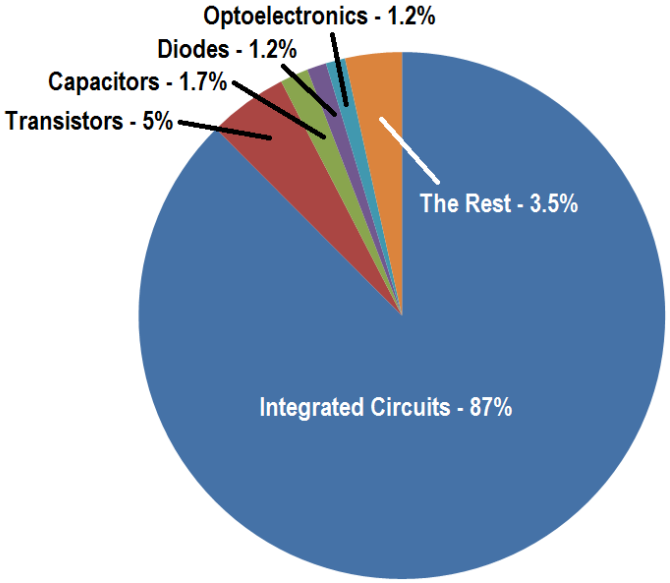


Figure 2: Breakdown of Counterfeit Electronic Parts

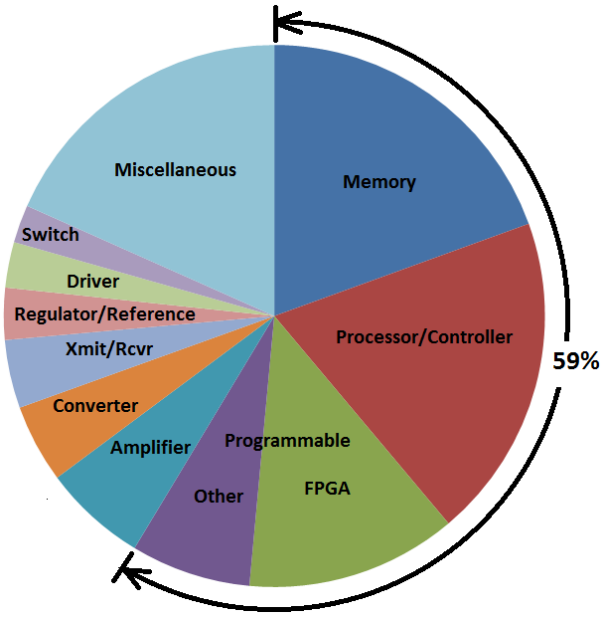


Figure 3: Breakdown of Counterfeit Integrated Circuits

- **Price and Volume** – Counterfeiters are much more likely to deal in materiel where a significant profit can be gained, either through a high purchase price or through large volume sales. High sale price items are targeted and listed at a discount to lure customers seeking lower purchase costs. Counterfeiters will often target materiel that is available in multiple quality levels, procuring low cost commercial items that can be remarked and sold at a higher price as industrial, automotive or military materiel.

- **Common Commercial Materiel** – Items commonly used in commercial applications are more likely to exist in high volume as electronic waste or e-waste. This is product that has been used in prior application, but has been reclaimed and refurbished. It may be resold as new product, although the materiel's reliability has likely been affected.

- **Strategic Value** – Materiel that presents specific strategic opportunity to an adversary may make for an attractive counterfeit target.

1.4 Supplier Risk

The strongest correlation between materiel and its likelihood of being counterfeit is the trustworthiness of the supplier. Regardless of supply class, purchase price, or other likelihood factors, purchasing materiel from an untrusted supplier increases the likelihood of purchasing counterfeit materiel. Part 2 of this Guidebook identifies specific criteria for identifying low risk suppliers.

1.5 Risk Assessment

Risk assessment is generally achieved by weighing the likelihood that an event will occur against the consequence of the occurrence. The 'five by five risk cube' in Figure 4 shows the interplay between the two factors. The green, yellow, and red boxes have been modified from the standard risk chart to reflect counterfeit materiel risk and inspection/test reaction. Table 1 shows

the recommended mitigation for each risk level. Table 2 explains how to select the likelihood rating (from A to E) based on supplier and type. NOTE: Any obsolete integrated circuit would be considered high risk materiel. Table 3 explains how to select the impact rating (from 1 to 5) based on system impact.

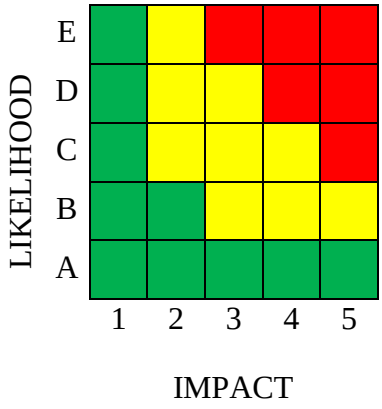


Figure 4: Risk Assessment Matrix

Table 1: Risk Mitigation

Risk Level	Recommended Mitigation
Green	No mitigation necessary
Yellow	Standard mitigation (inspection)
Red	Enhanced mitigation (inspection and test)

NOTE: Recommendation for enhanced mitigation above includes 'test'. For electronic parts, this may mean functional electrical test, or comparison of electrical signature with a known authentic electrical signature. For an assembly, it may involve electrical test and a search for malicious features. For other materiel, it may involve sample 'test to failure' (destructive) analysis to detect a weak component.

Table 2: Likelihood Assessment

Level	Supplier Type	Materiel Type
A	Authorized	All types
B	Unauthorized Approved	Low and medium risk materiel
C	Unauthorized Approved	High risk materiel
D	Unauthorized Unapproved	Low risk materiel
E	Unauthorized Unapproved	Medium and high risk materiel

Table 3: Impact Assessment

Level	Impact
1	Minimal or no system impact
2	Minor system impact
3	Moderate system impact
4	Major system impact
5	Safety or mission impact

Tables 2 and 3 are not hard requirements for completing the risk matrix, but are guidelines. The two biggest factors in implementing a mitigation plan are supplier type, and the materiel's criticality.

Part II: Supplier Selection and Procurement

Objective:

To identify how to assess and procure from low risk suppliers, and to mitigate risk if a low risk supplier is not available.

2.1 Introduction:

To minimize counterfeit risk, materiel should always be purchased from the OM or an authorized supplier when available. If an unauthorized supplier is the only available source, the supplier should be assessed to a set of criteria before being considered a low risk supplier. Acquisition procedures should allow the technical authority for each purchase to determine supplier suitability based on these criteria. Procurement procedures for high risk materiel should utilize an Approved Suppliers List (ASL) that is updated at least annually.

2.2 Supplier Types

SECNAVINST 4855.20 requires at risk materiel to be purchased from an authorized supplier whenever possible. If an authorized supplier is not available, materiel must be purchased from a supplier that meets appropriate counterfeit avoidance criteria, per industry standards listed in Appendix B. Defense Federal Acquisition Regulations Supplement (DFARS) section 246.870 outlines twelve "System Criteria" requirements for Cost Accounting Standards (CAS) covered contractors and their subcontractors, when buying electronic parts. These twelve requirements should be considered for any organization (not just a contractor), which buys materiel (not just electronic parts). As previously mentioned, the supplier type is the most critical factor in ensuring the purchase of authentic parts. There are four main types of suppliers. Descriptions of these four supplier types are listed in the following paragraphs.

2.2.1 Original Manufacturers

An OM is the organization which owns the design and/or engineers the materiel and has obtained the intellectual property rights. An OM typically provides a warranty for the materiel that not only includes replacement cost, but can include further assistance such as failure analysis, reliability data, and other support. This supplier type is the lowest risk possible. Materiel purchased from an OM has typically been produced completely within the manufacturer's controlled processes and facilities.

2.2.2 Aftermarket Manufacturers

An Aftermarket Manufacturer has obtained the rights from the OM to produce and sell replacement materiel. Usually the cause is the discontinuance of the materiel by the OM while a demand still remains. If the aftermarket manufacturer has obtained the intellectual property rights from the OM, then the risk of counterfeit is very low, similar to the risk of buying from an OM. Warranty from an aftermarket manufacturer is typically the same as from an OM.

2.2.3 Authorized Suppliers

Original and aftermarket manufacturers usually sell materiel through an authorized supply chain. An authorized supply chain can include authorized distributors, franchised distributors, sales representatives, etc. All of the suppliers obtain materiel directly from the OM or another authorized supplier, with a contractual agreement to do so. In the authorized supply chain the original/aftermarket manufacturer will honor the complete warranty. Authorized suppliers present a low risk for counterfeit materiel, although the risk is not as low as if the materiel is purchased directly from an original/aftermarket manufacturer.

An authorized supplier can be found by checking with the OM by either phone, email, or on the OM's website. The organization should not rely solely on the supplier's claim. It is possible for a supplier to be authorized for one OM's product lines, but not for another's, so care must be taken to confirm the authorization directly with the OM. It is the responsibility of the party which identifies the supplier (e.g., buyer, Requiring Technical Authority (RTA), Technical Point of Contact (TPOC)) to ensure that the lowest risk supplier type has been identified. Therefore, it is very important that these personnel have a solid understanding of the supplier types and the respective counterfeit risks.

2.2.4 Unauthorized Suppliers

An unauthorized supplier presents the highest risk for purchasing counterfeit materiel. These are suppliers that do not have a contractual agreement with an original/aftermarket manufacturer. Often the materiel obtained by an unauthorized supplier has not been contained within the authorized supply chain. Warranty for materiel purchased from an unauthorized supplier is typically for replacement cost only, and may be valid for a shorter time, 30 days or less. Materiel from unauthorized suppliers provides the greatest opportunity for counterfeiting. All materiel purchased from unauthorized suppliers should be considered at higher risk of being counterfeited.

Figure 5 provides a summary of the expected counterfeit risk based on supplier type. In this figure, the light green shading indicates lowest risk. The yellow shading indicates a slightly higher risk, while the orange shading notes the highest risk of using unauthorized suppliers. The overlap between authorized and unauthorized suppliers denotes the real world fact that some authorized supplies also sell materiel as an unauthorized supplier, and should be considered high risk when this is the case. The white vertical box titled "Approved Suppliers" denotes a government or contractor ASL. This is similar to the 'contractor-approved supplier' type mentioned in DFARS clause 252.246-7008. Most contractors' ASLs include OMs, authorized suppliers, unauthorized suppliers, value-added companies (e.g., replating, leadforming) and other company types. The different supplier types should be identified in the ASL so that the correct supplier type is used for each purchase.

Presence of an unauthorized supplier on an ASL does not relieve the buyer of the obligation to notify the contracting officer if buying materiel from that supplier.

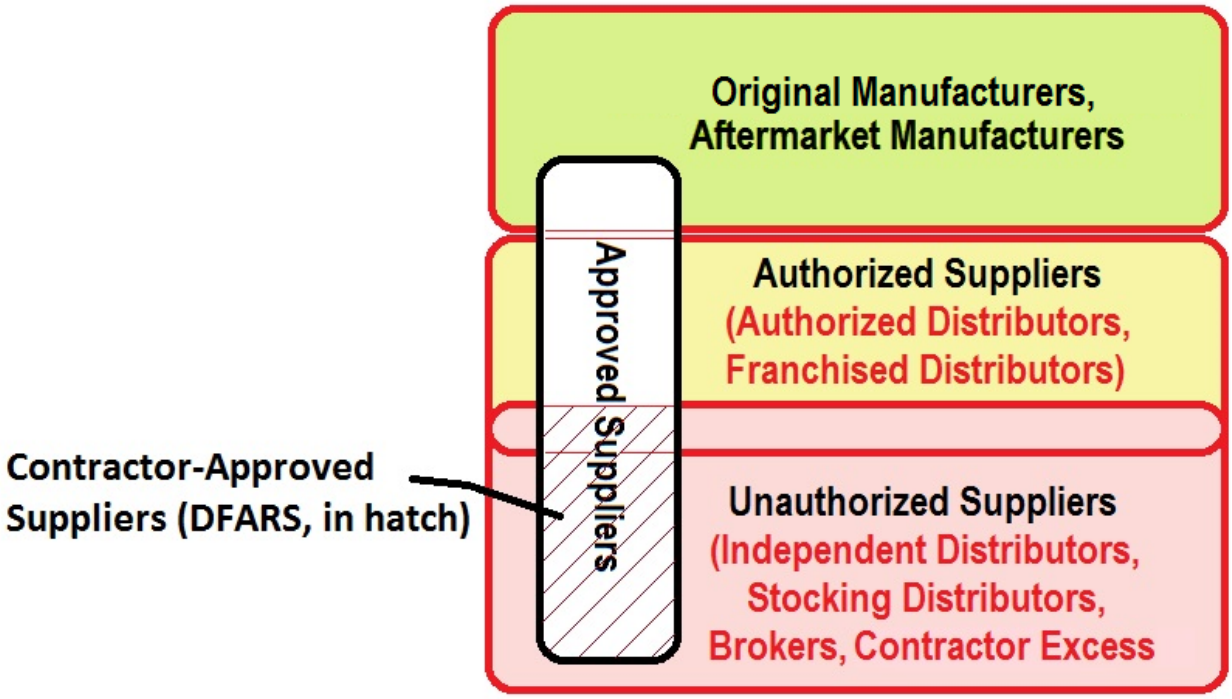


Figure 5: Supplier Types

2.3 Approving Unauthorized Suppliers

When an OM or authorized supplier is not available, the first option should be qualification of replacement materiel that is available from the authorized supply chain, or a redesign to eliminate the unavailable materiel. If this is not possible or feasible, then it may be necessary to purchase materiel from an unauthorized supplier. The TPOC, RTA, or whoever best understands the materiel's criticality should research unauthorized suppliers to ensure the materiel is procured from one who has implemented appropriate anti-counterfeit criteria. In order to streamline this research process for future procurements, an organization should maintain an ASL (updated annually), which includes approved unauthorized suppliers that have already been thoroughly assessed by the organization. These are suppliers that have been assessed to a set of anti-counterfeit criteria and determined to be low risk. DFARS counterfeit-specific clauses refer to these entities as contractor-approved suppliers, and the approval processes are subject to government review and audit.

Each organization (government and contractor) should maintain an ASL, and purchases from suppliers should be limited only to those suppliers that are on the ASL. For contractor-purchased materiel, each contractor should maintain its own ASL. The contracting officer may request the contractor's ASL periodically in order to review the selections. It is important to note that purchasing materiel from an unauthorized supplier on an ASL does not relieve the contractor or subcontractor from the requirement to notify the contracting officer per SECNAVINST 4855.20.

Assessments should always be conducted at the supplier's facility. Unauthorized suppliers are usually small businesses, and in general over ten percent of them are residential suppliers. Use of a mailed questionnaire will **not** provide protection against a supplier providing counterfeit materiel.

SAE ARP6178, "Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors," is an excellent tool for assessing unauthorized suppliers for electronic part purchases. The document contains an assessment tool with over 100 ratable questions which can be used to assess an unauthorized supplier's general anti-counterfeit processes (procurement, detection, containment reporting, etc.), with an associated score generated from the assessment. SAE AS6081, Fraudulent/Counterfeit Electronic Parts; Avoidance, Detection, Containment, and Mitigation – Distributors, also provides guidance on assessing unauthorized suppliers.

2.4 Alternative Unauthorized Supplier Approval Method

These requirements are best suited for application to electronic part suppliers, and may not be applicable to some mechanical part or material suppliers. It is recommended that as many requirements as possible are enforced, within the applicability and budget of the program, as these requirements are more stringent than current industry standards.

2.4.1 Supplier Assessment

The Supplier Under Assessment (SUA) should maintain its own approved supplier listing, hereafter referred to as the Supplier's Approved Supplier List (SASL). The SASL should have documented procedures to identify and differentiate between authorized and unauthorized suppliers. The assessor should check OM websites or with OM contact personnel to confirm selected SASL authorized suppliers are actually authorized.

The SUA should have documented procedures to ensure that, when possible, parts are obtained directly from an authorized supplier. In these cases, the SUA should provide traceability documentation proving this. The government or contractor has the right to contact the OM to confirm the validity of the traceability documentation.

2.4.2 Supplier Notification to Customer

If the SUA cannot obtain parts directly from an authorized supplier, the SUA should inform the government or contractor of this, and provide documented justification why the selected supplier is low risk, such as extensive past history of receiving authentic materiel. This notification and information should be provided at the time of quoting the materiel.

2.4.3 Supplier's Approved Supplier Listing

The SUA should maintain a listing of suppliers SASL. The listing should be maintained by a method that allows identification of dates when supplier status was changed (e.g., approved/removed, or reclassified within the listing). The SASL should have at least five different supplier levels defined. These levels, in order from lowest to highest risk, should include, but are not limited to:

1. Authorized. The supplier is contractually authorized by the OM to buy parts directly from the OM and sell parts to the SUA with full product traceability and warranty.
2. Preferred. The supplier has been fully assessed to this document or an applicable industry standard and passed the requirements along with any of the SUA's requirements. The supplier has been used for at least ten purchases by the SUA with no suspect or

confirmed counterfeit, or major nonconforming materiel detected. There are no outstanding quality or delivery issues.

3. Acceptable. The supplier has been fully assessed to this document or an applicable industry standard and passed the requirements along with any of the SUA's requirements. The supplier has not yet been used for at least ten purchases, but has had at least two purchases. There has been no suspect or confirmed counterfeit or major nonconforming materiel detected. There are no outstanding quality or delivery issues.
4. Probationary. The supplier has not been used for at least two purchases, or was previously listed Authorized, Acceptable, or Preferred, and has been downgraded due to significant quality or delivery issues identified by the SUA, GIDEP, or other industry databases. The supplier may regain Acceptable, Preferred, or Authorized status after a minimum of five authentic shipments to the SUA and resolution of any other issues, as well as a re-evaluation of the supplier. When a supplier has no prior transactions with the SUA, the supplier will also be considered as Probationary until providing at least ten shipments of authentic materiel with no major nonconforming materiel and no outstanding quality or delivery issues. A Prohibited supplier that has implemented acceptable corrective actions and been re-evaluated may be upgraded to this category.
5. Prohibited. The supplier has delivered suspect or confirmed counterfeit or major nonconforming materiel to the SUA, or has significant unresolved quality or delivery issues identified by the government, contractor, SUA, GIDEP, or other industry databases. This includes active suspensions or debarments indicated in the System for Award Management (SAM). A Prohibited supplier that has implemented acceptable corrective actions and been re-evaluated may be upgraded to Probationary. The SUA should never buy materiel from a Prohibited suppler.

2.4.4 Corrective Actions

The SUA should have in place a plan to require corrective actions if an Authorized, Preferred, Acceptable or Probationary supplier on the SASL is determined to have supplied suspect or confirmed counterfeit or major nonconforming materiel, including downgrading the supplier rating if necessary. Likewise, the government or contractor should require corrective actions from the SUA and potential removal from the ASL.

If an Authorized SASL supplier is classified Prohibited or removed from the Authorized SASL for shipment of suspect or confirmed counterfeit materiel (e.g., GIDEP or other industry alerts, government/contractor/SUA experience, SAM), the SUA should be required to review all prior purchases of materiel from that supplier for the last two years at a minimum, and determine whether testing was sufficient at the time to detect the reported method of counterfeiting. If the SUA previously purchased materiel from this supplier and inspection/testing is deemed insufficient, the in-house materiel should be re-authenticated. If additional materiel is determined to be suspect counterfeit, or if materiel is not available for re-authentication, the SUA should notify its customer in writing.

2.4.5 SUA Background

The SUA should be assessed periodically for indicators that the risk of counterfeit materiel is other than low. The assessment process should include, at a minimum:

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

2. Review “Contractor Profile Search” in the Product Data Reporting and Evaluation Program (PDREP).
3. Review of other peer databases for past unresolved quality issues if applicable (monthly as a minimum).
4. Review of SUA’s past history with the government or contractor, including quality or delivery problems (every three months as a minimum).
5. Review of Corrective Action Requests as necessary to upgrade/downgrade supplier.
6. Trade references (for initial screening).
7. Review of active suspensions and debarments indicated in SAM (every three months as a minimum).
8. Years in business (for initial screening).
9. Banking information (for initial screening).
10. Quality Management System certifications (annually).
11. Insurance and warranty (every six months).

The government or contractor should re-evaluate approved unauthorized suppliers before purchase, if six months have passed since the last purchase of parts from the supplier.

2.4.6 In-Stock Materiel

Materiel already in stock at the SUA’s facility may be used to fill orders. Materiel in stock which can be proven (i.e., traceability documentation) to have been purchased directly from the OM or an authorized supplier can be sold as authorized supplier materiel and be classified as authorized stock. If the materiel in stock was not bought directly from an authorized supplier, the parts should be considered unauthorized supplier parts. This includes contractor or government excess materiel which the SUA bought. Stock that was not bought directly from an authorized supplier should be classified as either stock confident or stock unknown. Stock confident is materiel which has passed all inspection and test requirements to an acceptable reporting format. Stock unknown is anything else. Stock materiel should be stored in a manner that does not reduce traceability (e.g., mixed or combined shipments).

2.4.7 Returned Parts and Restocking

Materiel returned to the SUA 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), the returned materiel should pass all inspection and test requirements, as well as have the expected lot and date code information confirmed.

2.4.8 Priority of Sale

The SUA should supply materiel in the order indicated in Table 4. If materiel is available both to purchase and from stock, and the order priority is identical, the Approved Supplier may choose from where to supply the parts.

Table 4: Order of Purchase, by Supplier or Stock Classification Status

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

For example, if materiel is available from a Preferred supplier and is also available as Stock Confident in the SUA's warehouse, either or both suppliers can be used to supply materiel. If, however, Authorized materiel is available either through purchase by the SUA or in stock, those parts should be first priority.

Stock Confident materiel can be provided without additional inspection and test, but the compliance report should be provided with the shipment. Stock Unknown parts should pass the inspection and test requirements and be upgraded to Stock Confident, before the materiel can be provided, with the corresponding report.

The SUA should notify the government or contractor in writing (including e-mail) if either of the following conditions is a necessary requirement to fulfill the sale:

- The order of preference specified in Table 4 will not be followed (e.g., Stock Confident is quoted instead of Authorized Stock).
- The SASL supplier will be Probationary.

2.4.9 Authentication of Materiel

All materiel purchased from the SUA that is not provided authorized (i.e., purchased directly from the OM or an authorized supplier) should undergo inspection and test. Refer to Part V for further information. All materiel not provided as authorized (i.e., purchased directly from the OM or an authorized supplier) should be inspected and tested to verify authenticity.

2.5 Procurement

When preparing a request for purchase from an unauthorized supplier, the TPOC, RTA, or whoever best understands the materiel's criticality should conduct market research on materiel suppliers utilizing the ASL or in accordance with documented supplier selection criteria.
The request for purchase should include the following as technical requirements for inspection and test (authentication) of materiel:

- Verifiable supplier testing capabilities
    - Laboratories are ISO 17025 and ISO 9001 certified

    - Lab personnel are IDEA-ICE-3000 certified (optional, and applies to electronic parts only)
- Ability to perform authenticity verification testing
- Ability to provide required inspection and test data report with materiel shipment
- Ability to provide photographs of the parts before procurement
- If possible, provide a manufacturer's warranty for the product and Certificate of Conformance (CoC) that traces the materiel to the OM

All procurement contracts should include clauses that allow for payment to be sent after materiel authenticity is investigated and for full refunds to be issued for any suspect counterfeit materiel. Even in the event of a refund, suspect counterfeit materiel should never be returned to the supplier. Suspect counterfeit materiel must be quarantined and disposed of so that it cannot re-enter the supply chain.

2.5.1 Acquisition Strategies

Purchases of materiel up to $3,500 can be completed by a certified Government Purchase Card holder. Therefore, a sole source can be pursued for these buys using OMs or their authorized distributors, whenever possible. If there are multiple authorized suppliers available, buys should rotate among the suppliers. If there are no authorized suppliers, then selection should be from an unauthorized supplier on the ASL. If there are recurring requirements for the same part, the buys should not be broken down into smaller increments to avoid higher threshold requirements.

For purchases less than $150,000 simplified acquisition procedures (SAP) are used. At least three suppliers should be provided by the technical authority (TPOC or RTA). Authorized suppliers should still be used as a first option. If unauthorized suppliers are the only option available, only approved unauthorized suppliers should be used. If there are not three low-risk suppliers available, the SAP Non-competition form can be used in these instances to ensure that critical and high risk materiel is procured from suppliers that are considered low-risk in terms of counterfeiting. The technical authority should identify any critical and high risk materiel in the data package provided to contracting.

Since many unauthorized suppliers are small businesses or other businesses identified for preferential sales (e.g., woman-owned, veteran-owned, historically underutilized business zone), it is often advantageous to buy materiel from unauthorized suppliers that is currently available from the authorized supply chain. It is very important to avoid the purchase of critical and high-risk materiel from unauthorized suppliers whenever possible. Therefore, usage of preferential supplier types should be limited to non-critical and low risk materiel.

For purchases greater than $150,000, Justification and Approval (J&A) for use of other than full and open competition can be used to ensure that materiel is purchased from the lowest risk supplier.

For General Services Administration acquisitions regardless of the dollar amount, a Limited Sources Justification can be used to ensure procurement only from low-risk suppliers.

Part III: Documentation

Objective:

To ensure the program's approach to counterfeit risk mitigation is documented appropriately.

3.1 Documentation

Each program is responsible for documenting critical materiel, materiel at high risk of counterfeiting, and counterfeit mitigation processes within the appropriate program plans. DON programs are not required to develop a formal counterfeit materiel program plan; however, counterfeit detection and avoidance processes should be integrated into the appropriate program plans to the degree identified in the program's risk assessment, including the:

- Risk Management Plan (RMP): The RMP should include the specific requirements and criteria to assess the risk of materiel to counterfeiting, which is based on criticality of the part and criticality in its application. It should identify and document anti-counterfeit risk mitigation actions for materiel identified as critical or having a high risk of being counterfeited.
- Systems Engineering Plan (SEP): The SEP should reflect how materiel assessed to be at risk for counterfeiting is managed during design and production, such as a robust Parts and Materiel Management Plan (PMMP).
- Program Protection Plan (PPP): The Department of Defense (DoD) PPP Streamlining guide provides information on what should go into the PPP. Supply chain management risks related to Program Protection are defined in DODI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks.
- Life Cycle Sustainment Plan (LCSP). The LCSP should include information on the process for selecting, procuring and testing materiel identified as high or moderate counterfeit risk during sustainment. It can point to other documents as necessary, such as the PMMP if applicable.
- Diminishing Manufacturing Sources and Material Shortages (DMSMS) management Plan. The Assistant Secretary of the Navy Research, Development and Acquisition (ASN(RD&A)) DMSMS Management Plan Streamlining Guide, dated July 2016 should be used to develop the program's DMSMS Plan. While planning for DMSMS, the program should understand that the most common situation in which suspect counterfeit materiel is encountered is in obsolescence, when the materiel is no longer available from the OM or an authorized supplier. Most counterfeit materiel in the supply chain is purchased from a supplier not authorized to supply the OM's materiel. These unauthorized suppliers are commonly referred to as independent distributors or brokers. Although there are slight differences between the names, in this document independent distributors, brokers, non-franchised suppliers, will all be referred to equally as unauthorized suppliers. Counterfeit mitigation processes should be fundamentally integrated into a proactive and robust DMSMS management process. Because of the much higher risk of receiving counterfeit materiel when buying from unauthorized suppliers, materiel should always be purchased from the OM or an authorized supplier whenever possible. While materiel from unauthorized suppliers is often cheaper, the cost of authentication work (e.g. inspection and test) may offset any savings. In addition, the

replacement costs for installed materiel far exceed the original cost, without even considering potential risks to life and mission. Any DMSMS resolution that includes purchasing material from unauthorized suppliers should factor in the additional costs of authentication and risk of installing counterfeit parts.

- Parts, Materials, and Processes Management Plan (PMPMP): The PMPMP documents the processes used to minimize the risk of procuring and/or using counterfeit parts and materials. The PMPMP should specifically address counterfeit parts and materials prevention and detection methodologies. These methodologies should include, as a minimum:
  - Maximizing availability of authentic, originally designed and/or qualified parts throughout the product's life cycle, including management of parts obsolescence
  - Assessing potential sources of supply to minimize the risk of receiving counterfeit parts or materials
  - Maintaining a listing of approved suppliers with documented criteria for approval and removal of suppliers from the list
  - Certificate of compliance and supply chain traceability for all electronic part purchases
  - Minimum inspection and test methods to detect potential counterfeit parts and materials per Part V of this document
  - Training of personnel in counterfeit avoidance and detection practices
  - Flow down of counterfeit parts and materials prevention and detection requirements to subcontractors
  - Reporting counterfeit parts and materials to other potential users and Government investigative authorities

Part IV: Contracting

Objective:

To provide information on what requirements and information the contract should contain to minimize the risk of counterfeit materiel in DON systems or the supply chain.

4.1 Process:

DON policy requires that DFARS subpart 246.870, Contractor Counterfeit Electronic Part Detection and Avoidance, is enacted for all applicable procurements (i.e., electronic parts and assemblies). For procurements where DFARS 246.870 does not apply (i.e., non-electronic materiel), DON policy ensures that solicitations require contractors (and their subcontractors at all tiers flow down requirements) who obtain critical or high risk materiel to implement a risk mitigation process as follows:

- If the materiel is currently in production or currently available, solicitations shall require the materiel to be obtained only from authorized suppliers
- If the materiel is not in production or currently available from authorized suppliers, solicitations shall require the materiel to be obtained from suppliers that meet appropriate counterfeit avoidance criteria
- Require the contractor to notify the contracting officer when critical or high risk materiel cannot be obtained from an authorized supplier
- Require the contractor to take mitigating actions to authenticate the materiel if purchased from an unauthorized supplier
- Require the contractor to report instances of counterfeit and suspect counterfeit materiel to the contracting officer and the GIDEP as soon as the contractor becomes aware of the issue

4.2 Defense Federal Acquisition Regulation Supplement

The DFARS provides contract clauses to assist in the prevention of counterfeit electronic parts from entering systems in production as well as into the supply chain. The following provides a brief synopsis of DFARS clauses that apply:

- DFARS 246.870: Prescribes policy and procedures for preventing counterfeit electronic parts and suspect counterfeit electronic parts from entering the supply chain when procuring electronic parts or end items, components, parts, or assemblies that contain electronic parts.

    - DFARS clause 252.246-7007: Contractors that are subject to the cost accounting standards (CAS-covered contractors) and that supply electronic parts or assemblies, and their subcontractors that supply electronic parts or assemblies, are required to establish and maintain an acceptable counterfeit electronic part detection and avoidance system.

- DFARS clause 252.246-7008: If a contractor is not a CAS covered contractor, then DFARS clause 252.246-7008 applies and establishes risk-based purchasing, traceability, and notification requirements for contractors that supply electronic parts or assemblies, and their subcontractors that supply electronic parts or assemblies.

Appendix C highlights additional clauses of the DFARS that are applicable to this document.

4.3 Government-Industry Data Exchange Program

All domestic contractors should be GIDEP members. As GIDEP members, they should periodically review new GIDEP reports for counterfeit materiel. The review should include checking for reported counterfeit part numbers used in the contractors' (or subcontractors') systems, as well as whether the reported supplier has provided prior materiel to the contractor that may not have been authenticated per industry or Department of Defense (DoD) adopted standards.

- GIDEP can be accessed at https://members.gidep.org/gidep.htm. The following Data Item Descriptions (DIDs) are active and may be used for including GIDEP in contracts:
  - GIDEP Annual Progress Report DID: DI-QCIC-80127A
  - Alert/Safe-Alert DID: DI-QCIC-80125B
  - Response to an Alert/Safe-Alert DID: DI-QCIC-80126B

4.4 Statement Of Work

While the DFARS provides some standard protections against counterfeits, the Statement of Work (SOW) should include additional safeguards tailored to the risk and type of materiel. The following provides guidance on creating SOW information. Appendix D includes sample language that should be considered for inclusion in the SOW to cover all materiel. The following contractual processes are required as identified in SECNAVINST 4855.20:

1. Materiel that is either in production or currently available must be purchased from an OM, aftermarket manufacturer, or other authorized supplier.
2. Materiel that is neither in production nor currently available may be purchased from suppliers, including unauthorized suppliers, that meet appropriate counterfeit avoidance criteria documented in industry anti-counterfeit standards.
3. In cases where the supplier is not authorized, the contractor must notify the contracting officer, and authenticate the materiel.
4. The contractor must report all suspect and counterfeit materiel to the contracting officer and to GIDEP.

While a counterfeit prevention plan is not required by the government, the contractor should be required to implement and maintain such a plan, based on counterfeit risk. DID DI-MISC-81832, Counterfeit Prevention Plan, describes the minimum requirements all contractors should document in their Counterfeit Prevention Plan, including processes for procurement, supplier selection, monitoring and detection, reporting, and self-auditing. It is vital that this plan include requirements and enforcement protocols for all critical subcontracts and subcontractors.

Part V: Detection

Objective

To provide information on when to authenticate materiel required processes to use, and how to determine if materiel is likely counterfeit.

5.1 Process:

Basic detection techniques should be an integral part of the procurement and receiving processes. Any critical materiel purchased from an unauthorized supplier should be subjected to inspection and/or test to provide an acceptable level of confidence in materiel authenticity. Materiel criticality and the acceptable level of risk, as determined by the program office (TPOC, RTA, or whoever best understands the materiel's criticality), will determine the level of inspection and/or testing rigor required. The failure analysis process should include the analysis for counterfeit materiel, especially for recurring trends or unexpected low reliability.

5.2 When to Use Detection Protocols

In the event a low risk supplier cannot be used, mitigating actions to authenticate the materiel through inspection and/or test must be taken to determine whether the materiel is likely counterfeit. Basic counterfeit detection techniques, such as verifying consistency within paperwork and visually inspecting materiel and its packaging, should be integrated into the receiving process for all materiel regardless of the supplier. For materiel that is considered high risk, counterfeit detection techniques tailored to the materiel type should be performed before the materiel is deemed acceptable to place into the DON supply chain. Appendix E provides a suggested flow, based on risk and criticality, for determining the level of authentication work, if any, should be performed on materiel. Industry standards provide guidance regarding detection of counterfeit materiel, including recommended inspections and tests, sample sizes, indicators that the materiel is counterfeit, etc. Appendix B contains a list of these industry standards.

5.2.1 Electronic Parts

Functional testing (e.g., parametric testing) is an excellent method for detecting counterfeit electronic parts, but may not be sufficient to guarantee authenticity. For integrated circuits, most counterfeits actually contain the correct die, or at least a die with the same functionality as the authentic part. The 'die' of an electronic integrated circuit is the small electronic design within the package, which contains all of the functionality of the part (see Figure 6). The rest of the package serves to encase or protect the die, dissipate heat, and bring the die connections external to part. Counterfeit electronic parts with the same die may pass functional testing. With the risk of chemical, thermal, mechanical or electrical damage through uncontrolled handling, there is a greater chance that electronic parts will have a reduced life span.

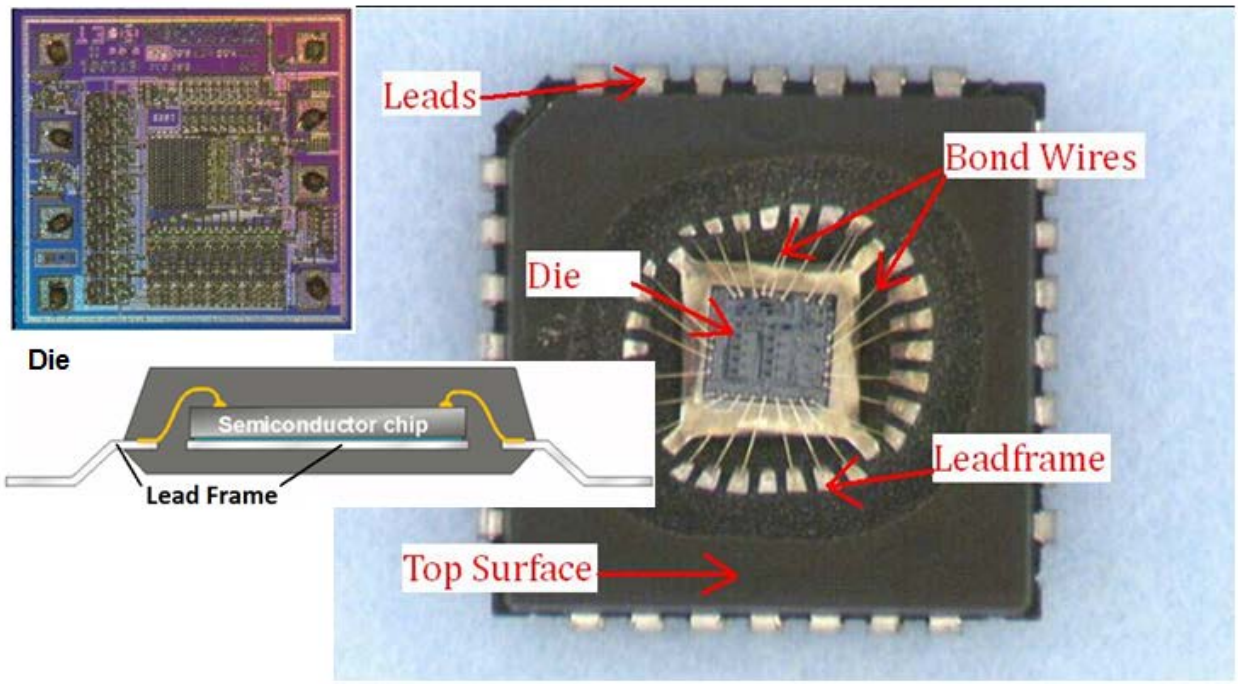


Figure 6: Overview of Integrated Circuit

For electronic parts, DFARS clause 246.870 directs the use of industry standards in the inspection and test (generally termed 'authentication') of electronic parts that were purchased from unauthorized suppliers. SAE AS5553, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition, lists SAE ARP6328, Guideline for Development of Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition System for guidance on the applicable tests. Since ARP6328 is a guidance document, DON organizations should not reference this document unless all desired inspections and tests are specifically noted as requirements in the SOW.

A preferred standard is SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors. This document provides the best suite of inspections and tests for electronic parts. Appendix F contains a listing of indicators that an electronic part may be suspect counterfeit. Appendix G contains examples of counterfeit electronic parts with the detection method indicated.

5.2.2 Mechanical Parts and Materials

SAE AS6174, Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel, is the standard devoted to the avoidance and detection of mechanical parts and materials.

Counterfeit mechanical parts and materials may also be detectable through the use of a core set of techniques. However, the core set is more diverse than for electronic parts, and it can vary widely from one materiel type to another. There is no core set of inspections and tests that are applicable across the board. Table 5 lists examples of the equipment and test methods that are useful in the detection of counterfeit mechanical parts and materials. Appendix H contains a

listing of indicators that a mechanical part or material may be suspect counterfeit. Appendix I contains examples of counterfeit mechanical parts and materials.

Material Visualization and Measurement	Alloy/Material Identification	Heat-Treatment/Finish Identification
• Stereo microscope • Optical microscope • Digital microscope system • Scanning electron microscopy (SEM) • Non-contact measurement system • Contact coordinate measuring machine (CMM) • Profilometer	• Scanning Electron Microscope-Energy Dispersive Spectroscopy (SEM-EDS) • X-ray Fluorescence Spectroscopy (XRF) • Also capable of non-destructive film thickness measurements • Induction Coupled Plasma Atomic Emission Spectroscopy (ICP-AES) • Fourier Transform Infrared Spectroscopy (FTIR) • X-ray photoelectron spectroscopy (XPS)	• Mechanical cross-section grinding and polishing • Chemical and thermal etching of microstructure • Rockwell Hardness, scales A, B, C, D, and superficial • Micro Hardness, Knoop and Vickers

Table 5. Example Test and Equipment for Detection

5.3 Independent Authentication

There are a relatively small number of counterfeit detection laboratories in the United States that can authenticate suspect electronic parts, and even fewer capable of detecting counterfeit mechanical parts or materials. Another option is to use a trusted, capable DOD or DON laboratory to authenticate the materiel. There are a few standards which address qualification of lab personnel and equipment, such as ISO 17025, General requirements for the competence of testing and calibration laboratories. In addition, SAE AS6171 contains guidance on the certification and training requirements for various anti-counterfeit inspection techniques.

Regardless of the chosen laboratory, it is critical to ensure the inspections and tests were performed thoroughly. The lab should be required to provide a report which contains photographs of the materiel before and during analysis, photographic documentation of any indicators found, and a summary opinion on the authenticity of the materiel. Any report which documents the materiel's authenticity in simple pass/fail fashion should be considered unacceptable.

If the selling company (unauthorized supplier) has been thoroughly assessed and found to be trustworthy, the program may decide to rely on the supplier's own authentication work. As mentioned above, all inspection and test work should be documented and reported in a manner which allows the program to plainly see:

- All inspection and test results (i.e., photos, tables, charts)
- Which tests were performed
- The sample size

- A summary conclusion on the materiel's authenticity
- Visual documentation will allows the reviewer to reach the same conclusion as the authentication facility

This is especially true for reports in which the materiel has been assessed as authentic.

5.4 Supporting Information

In support of authentication efforts, the following information should be gathered to capture a complete profile of the materiel to be examined:

- Part numbers/lot numbers/date codes of materiel
- OM technical specifications
- Industry reports (e.g., GIDEP, PDREP)on the materiel and supplier
- Sample size available for authentication, if required
- Availability of known good (authentic) materiel, against which the suspect materiel can be compared
- Part history (part or system test results or failures) if available

Each lot, batch, or date code should be authenticated as a separate authentication lot. An authentication lot is defined as one shipment of a specific lot, date code, batch number, or other group identification. For example, a single part number shipment which contains four different lot numbers (of the same part number) should be treated as four separate authentication lots. Likewise, the receipt of materiel with the same part, lot, and batch numbers should be considered three separate authentication lots if the materiel is received in three separate shipments from the supplier.

5.5 Basic Detection for All Materiel

Although authentication of suspect materiel might require a wide variation in inspection and test, there are some commonalities in the preparation and authentication process. In addition to the guidance provided in appendices F, G, H, and I, IDEA-STD-1010, Acceptability of Electronic Components Distributed in the Open Market, provides additional valuable guidance for detecting counterfeit electronic parts.

There is also a significant variation in materiel counterfeit indicators. An indicator is considered to be any observation during authentication that causes the inspector to question if the materiel is authentic. These can range from minor indicators - such as chips in the package on an electronic integrated circuit, or sanding marks on a mechanical fastener – to major indicators such as multiple die designs in the same integrated circuit lot, or the wrong plating or anodization on a washer. The best two methods to confirm that suspect materiel is counterfeit are to:

1 Document multiple indicators that the materiel is counterfeit.
2 Obtain the OM's analysis and response that the materiel is likely counterfeit.

An OM's conclusion that the materiel is likely counterfeit provides the best confidence of all indicators. Documentation of multiple indicators not only increases confidence that materiel is counterfeit, but the absence of indicators in a thorough authentication effort increases the confidence the materiel is safe to use.

5.5.1 Documentation Inspection

The first checkpoint in the detection of counterfeit materiel is the inspection of all paperwork (including packaging and part labels) which accompanies the shipment. Depending on the materiel, the documentation should provide:

- The origin of the shipment
- Certification of any special testing or screening
- Any authentication testing performed by the supplier
- Date codes, lot codes, quantity, etc.

Documentation should be closely examined to see if anything is missing or suspicious. Suspicious information includes, which is not limited to misspelled words, inaccurate logos, inaccurate bar codes, poor grammar, etc. Missing or suspicious information can be based on previously received documentation for the same materiel.

Categories and indicators of counterfeit documentation include the following:

1. Altered Documents
   - Excessively faded or unclear or missing data
   - Use of correction fluid or correction tape
   - Type style, size or pitch change is evident
   - Data on a single line is located at different heights
   - Lines on forms are bent, broken or interrupted indicating data has been deleted or exchanged by “cut and paste”
   - Handwritten entries are on the same document where there is typed or preprinted data
   - Text on page ends abruptly and the number of pages conflicts with the transmittal

2. Signatures and Initials
   - Corrections are not properly lined-out, initialed and dated
   - Document is not signed or initialed when required
   - The name of the document approver, or title, cannot be determined.
   - Approvers name and signature do not match
   - Document has missing or illegible signature or initials

3. Certification
   - Technical data is inconsistent with code or standard requirements
   - Certification/test results are identical between all tested item, normal variation should be expected
   - Documentation Certificate of Conformance and Testing is not delivered as required on the purchase order, or is in an unusual format
   - Document is not traceable to the items procured

5.5.2 Materiel Inspection

Once the documentation has been examined, the materiel itself must be inspected for indicators that might raise suspicion. Some indicators provide a high level of confidence that the materiel may be counterfeit (e.g., mixed internal designs in the same package, non-magnetic materials attracted to a magnet), while other indicators (smudged markings, chips and scratches) might be

a result of processing, handling, or other processes which can be, but are not always, counterfeit indicators.

5.6 Counterfeit Materiel Detection

As mentioned previously, counterfeit detection techniques cannot guarantee materiel authenticity. However, a relatively small suite of tests can be used to detect counterfeit electronic parts due to similarities in packaging and function. These basic tests are documented in SAE standards AS5553, AS6081, and AS6171. The tests were chosen for the fairly wide range of detectability achieved when the whole suite of tests are performed. In cases of highly critical electronic parts or parts at higher risk of malicious counterfeiting, additional tests may be warranted, such as functional electrical test or comparative analysis of basic electrical responses.

The testing required to detect counterfeit mechanical parts and materials is dependent on the critical properties of the part or material. Standards and engineering drawings should be referenced to determine applicable tests for a given materiel. For example, alloy composition requirements can be verified by a number of chemical analysis techniques including X-Ray Fluorescence (XRF), Energy or Wavelength Dispersive Spectroscopy (EDS/WDS), or Inductively Coupled Plasma Atomic Emission Spectroscopy (ICP-AES). Heat treatment conditions can be verified using mechanical or hardness testing. Plating thickness and composition can be verified through cross section or XRF. Tests can range from non-destructive to destructive. If a specific materiel is required for a critical application, it is a best practice to use applicable testing in the specification to ensure that the specific materiel was received.

5.6.1 Detection Methods for Assemblies

Entire electronic assembles and commercial items can also be susceptible to counterfeiting. Many overall visual inspection indicators (documentation, labeling, markings, etc.) apply to assemblies. Comparison to a known good assembly or input from the OM would also be beneficial. Equipment may be labeled with serial numbers that the OM can verify. Another technique is to disassemble the item into its subcomponents and apply standard counterfeit inspection tests on the individual components of the assembly. It should also be verified if possible that the manufacturing dates of the subcomponents were prior to the manufacturing date of the assembly. It is also important to consider the firmware that may be part of an assembly. It should be verified that the correct version of the firmware is installed on the assembly.

5.6.2 Detection Methods for Information and Communications Technology (ICT) Equipment

ICT manufacturers sell their equipment globally. Often the pricing in other countries is lower than the domestic pricing. This price differential creates incentives for a grey market on ICT equipment. The OM will often not provide support for products sold in other countries as it may violate licensing agreements. Detection methods applicable to commercial items may be applied to detect counterfeit grey market product. This product should be avoided by purchasing equipment from authorized suppliers. Appendix D provides sample language to include in Requests for Quote (RFQ) or SOWs to avoid purchasing grey market ICT equipment. When purchasing ICT equipment, ensure that the seller provides a full manufacturer's warranty as well as valid software licenses if applicable.

5.6.3 Hardware Assurance

Traditional counterfeit detection methods may not be able to detect whether the parts have been tampered with in malicious ways. It is recommended that programs develop and implement a process for mitigating risks associated with malicious hardware designs, modifications or code insertion for critical hardware. Parts with programmable logic or memory may be particularly susceptible. Methods for mitigation should also address firmware integrity. High risk parts with suspect and/or detected risks should be referred to the Joint Federated Assurance Center (JFAC) for further validation and verification. The JFAC was established by the Office of the Secretary of Defense (OSD) to ensure DOD organizations jointly develop capabilities to support the trusted defense system needs, in order to ensure software and hardware security.

5.6.4 Authenticity of Defense Logistics Agency Electronic Parts

The DLA enacted measures in 2011 to authenticate certain high-risk parts maintained within DLA storehouses. This Federal Stock Classification (FSC) category is 5962 (Electronic Microcircuits). DLA instituted a requirement to mark all of the parts with a deoxyribonucleic acid (DNA)-based ink which fluoresces under examination by ultraviolet light. This marking signifies the parts were bought from an authorized supplier, or adequate authentication analysis has been performed. All 5962- parts purchased from DLA should be checked to ensure the DNA ink marking is present. Failure to detect this ink might be an indicator the parts were procured by DLA before enactment of this marking, and that these parts should be authenticated if DLA purchased them from outside the authorized supply chain.

DLA maintains a Qualified Suppliers List for Distributors (QSLD). This listing, which includes authorized and unauthorized suppliers, verifies distributors have a Quality Management System (QMS) in place to minimize counterfeit risk for electronic parts in FSC 5961 and 5962. DLA has QSLD listings for other materiel as well, including mechanical parts.

DLA also maintains a Qualified Testing Suppliers List (QTSL) which establishes QMS and inspection/test requirements for FSC 5961 and 5962 electronic parts. The authentication requirements are based on SAE AS6081. The QSLD and QTSL listings form a core part of DLA's counterfeit mitigation efforts.

5.6.5 Stockroom Sweeps

One of the biggest concerns within DON is for materiel that was purchased before there was significant awareness of counterfeit risk. Some of this materiel was likely purchased from unauthorized suppliers, and placed into the stockroom with no authentication performed. It is important to attempt to identify and authenticate this materiel. A suggested method is to:

- Search the approved supplier listing for high-risk suppliers (NSWC Crane maintains a listing of these suppliers, based on government and industry databases)
- Identify materiel purchased from these high-risk suppliers
- Determine which of the purchased materiel is at high risk for being counterfeited
- Determine the criticality of this materiel to the end use application
- Develop an authentication plan for the high-risk critical materiel procured from high-risk suppliers

5.7 Failure Analysis

The potential for counterfeit materiel should be considered during all levels of failure analysis. Failure analysts should be trained on common counterfeit indicators pertaining to the particular materiel technology being investigated. Counterfeit detection investigations should be formally implemented when a recurring failure trend or unexpected behavior is observed in materiel with questionable procurement history. This is particularly important for critical materiel but should be practiced whenever possible.

5.8 Determination of Suspect Counterfeit

During the authentication process, it is not uncommon for minor counterfeit indicators to be identified. The distinction between 'counterfeit' and 'authentic' is sometimes not obvious, as minor indicators, such as documentation errors or scratches and other marks, can be present in authentic materiel. Since obsolescence drives the buyer to high-risk suppliers, the materiel is more likely to have been stored for a longer period than materiel still in production, and may have changed hands several times. These handling and storage processes increase the likelihood the materiel is no longer in pristine condition. Therefore, care should be taken to perform enough authentication work to determine authenticity with a reasonable level of confidence. The two best methods by which to determine materiel is suspect counterfeit are to:

1. Identify multiple suspect counterfeit indicators.
2. Obtain information from the OM to support that it is counterfeit.

Appendices F and H list many of these indicators, along with a minor, moderate, or major significance, defined as follows:

- Minor indicator - sign of quality or handling issues that might not be related to counterfeiting
- Moderate indicator - definite cause of suspicion for the part's authenticity
- Major indicator - strong risk that the part has been modified and qualifies as counterfeit

Using the above as a basis for assigning significance, a threshold for reporting materiel to PDREP and GIDEP as suspect counterfeit would occur if any one of the following conditions is true:

- One major indicator and one moderate indicator
- Three or more moderate indicators
- Two or more moderate indicators and two or more minor indicators

If during the authentication, the indicator values add up to suspicion of counterfeit the materiel can be classified as suspect counterfeit, and ideally the materiel should be inspected or tested further in order to increase confidence in the ruling.

Part VI: Containment, Disposition and Reporting

Objective

To provide information on appropriate containment, disposition, and reporting processes when materiel is identified as suspect counterfeit.

6.1 Containment

Suspect counterfeit materiel should be impounded, along with all other items from the same lot and date code. This includes uninstalled (stock and production floor) materiel, materiel installed into hardware, and may include in-process or finished assemblies, including product that has already been shipped to the customer for further processing or final installation. Mitigation steps include:

- Notify the program office, contracting officer, and NCIS immediately when suspect counterfeit materiel is identified
- Secure the materiel and mark external packaging to denote it is suspect counterfeit to prevent it from re-entering the supply chain
- Under no circumstances should suspect counterfeit materiel be returned to the supplier, even if this refusal results in lost reimbursement costs. Do not contact the supplier about the suspect counterfeit materiel. Requests for analysis should be referred to the OM
- As part of the containment process, personnel should determine the possibility of additional counterfeit materiel by investigating prior purchases of:
    1. Any materiel from that supplier, and
    2. Purchases of the same lot and date code from other suppliers.

All potential hardware items with the suspect materiel should be identified, and the users notified.

6.2 Disposition

Suspect or confirmed counterfeit materiel cannot be scrapped or otherwise disposed of without approval from investigative authorities and legal (if involved) or the contracting officer. Materiel should be provided upon request to investigative agencies for ongoing investigation or prosecution. As detailed earlier, suspect or confirmed counterfeit materiel should not be returned to the supplier or handled in a way which would allow its resale or reuse.

Upon authorization to release suspect materiel by the cognizant program office and/or legal authorities, the materiel must be destroyed to prevent reintroduction into the supply chain. Methods to destroy materiel may include, but are not limited to, shredding or crushing of small electronics and parts and drilling of pressure containing parts to purposely breach the pressure boundary.

Counterfeit materiel represents a performance risk that is impossible to quantify, since the materiel may have been exposed to unquantified stresses (mechanical, thermal, electrical, chemical, etc.) or be functionally inferior to its advertised capabilities (designed and tested to a lesser specification). For this reason, suspect counterfeit materiel should be removed and

replaced. However, there are other factors, such as cost, schedule, confidence, and criticality that can impact this decision. Figure 7 shows a suggested flow for determining whether or not to replace fielded suspect counterfeit materiel. This example flow shows how criticality, tampering, replacement costs, failure history, and materiel analysis can play a role in mitigation of suspect counterfeit materiel.

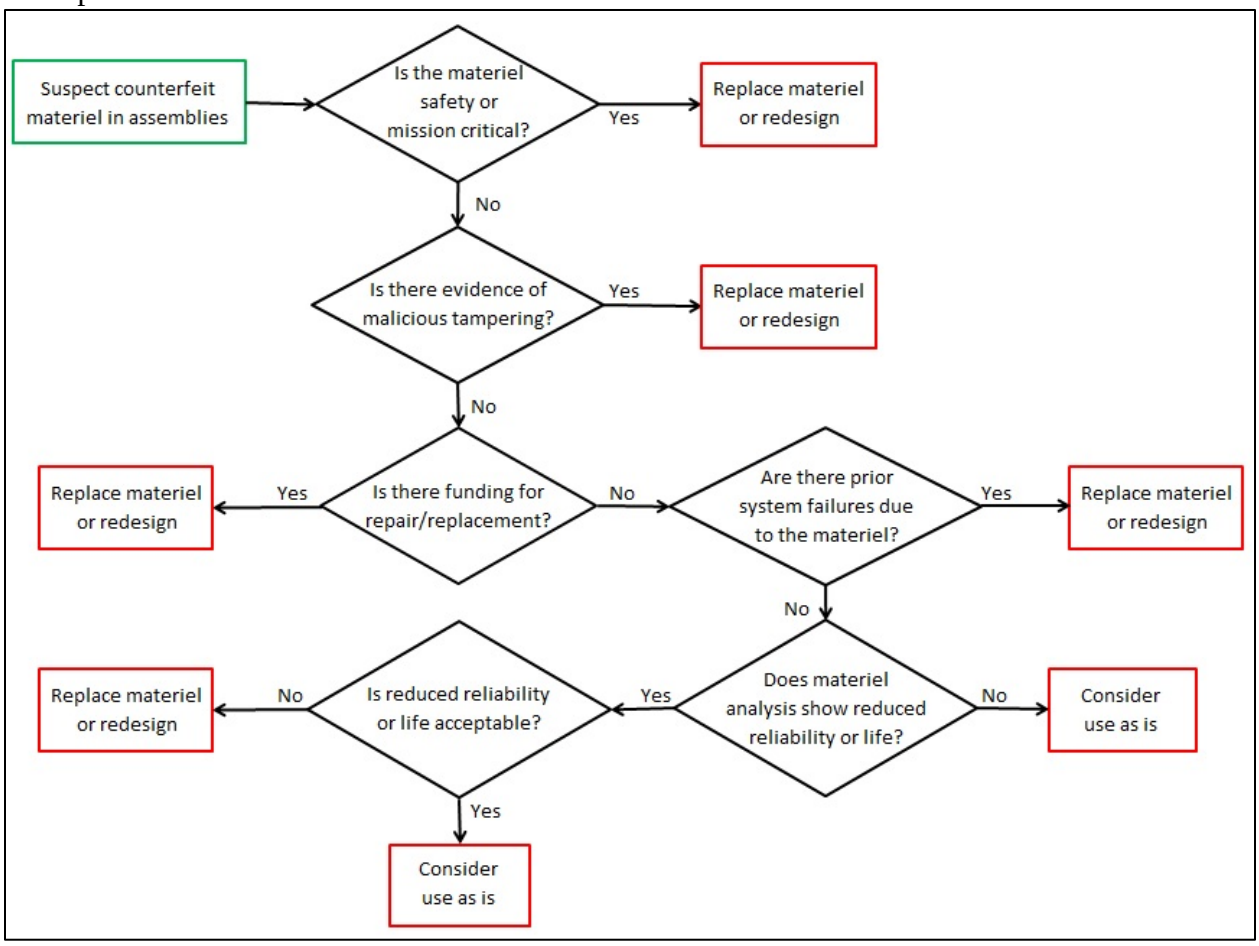


Figure 7: Disposition Decision Tree

6.3 Reporting

Each occurrence of suspect counterfeit materiel must be reported to NCIS, Navy Assistant General Counsel Acquisition Integrity Office, the contracting officer, the pertinent chain of command, and all users of the materiel. Counterfeit and suspect counterfeit materiel should be reported in PDREP using a PQDR. The PDREP website has guides, manuals and training about how to fill out and input these reports. When generating a PQDR for suspect counterfeit materiel, the appropriate Detailed Cause Code is "5AS-COUNTERFEIT MATERIEL, SUSPECT". The originator can send the PQDR to a screening point, action point, or support point for further analysis. NAVSO P-3683 and DLA Regulation (DLAR) 4155.24 details the process for reporting in PDREP and describes the responsibilities of the originator, screening point, action point and support point. PDREP can be accessed at https://www.pdrep.csd.disa.mil. The EZ PQDR module can be accessed without a common access card.

Reports should be filed with GIDEP within 60 days, unless told otherwise by investigating authorities. All counterfeit and suspect counterfeit materiel "affirmed" 5AS Suspect Counterfeit Materiel PQDRs should be forwarded to GIDEP using the tool in PDREP by the PQDR Action Point, per DLAR 4155.24.

This page intentionally left blank

Part VII: Contractor Assessment

Objective

To provide guidance on how to assess contractor anti-counterfeit processes, and determine the risk for installing counterfeit materiel in DON systems.

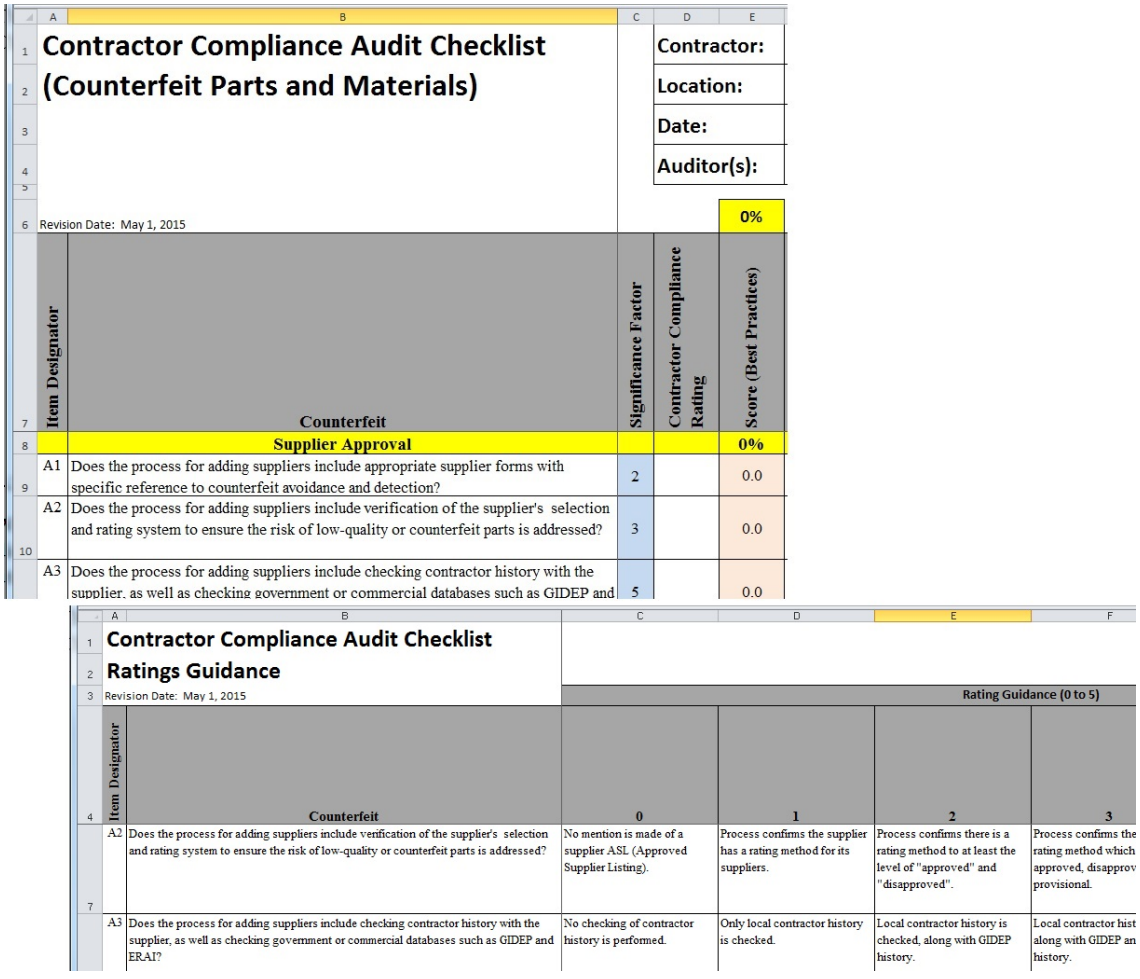
7.1 Contractor Assessment

Auditing of critical contractors should be determined by the program office, contracting officer, or system engineering. Critical contractors and subcontractors should be audited at least once before full-rate production, in order to assess the risk of counterfeit materiel to the system. Use of Defense Contract Management Agency audit results can help in determining the acceptability of a contractor's supplier selection or overall anti-counterfeit processes. Often during contract negotiations the contractor may seek to adjust, or 'tailor' certain contractual requirements, citing prohibitive implementation costs. Before any adjustment is granted, it is crucial to consider mission and safety criticality, as well as the requirements mentioned in DFARS clause 246.870.

There is a useful tool developed by the Missile Defense Agency (MDA) to assess a contractor's anti-counterfeit processes. This tool is a checklist with nearly 60 rateable questions, in eleven different categories such as supplier approval, supplier selection, detection, handling, reporting, training, etc. When completed, each section is scored from 0 to 100 percent as an indicator of the contractor's adequacy. There is also an overall score. Guidance on how to score each question is provided in the file, so that scoring can be consistent and repeatable. Since the scoring is based on industry best practices instead of specific DOD requirements, a score of 70 percent usually indicates an adequate anti-counterfeit program. Overall scores under 50 percent are an indication of significant weakness in the contractor's anti-counterfeit program. Figure 8 lists the breakdown of questions by category, while Figure 9 shows a partial image of the checklist and guidance. The full checklist with guidance is included in Appendix J. For large DON programs (over one hundred contractors and subcontractors), it is generally not feasible to audit all of the supply chain. In choosing which contractors to audit, the main considerations should be 1) criticality of the systems, 2) past performance in counterfeit mitigation, and 3) documented flow down issues.

	Rateable Questions	Significance Factor					
Category	#	N/A	2	3	4	5	10
Supplier Approval	12		1	5	1	5	
Supplier Selection	9			2		6	1
Detection	7			1	2	1	3
Handling/Storage/Trace/Test	4			1	2	1	
Containment	4	1			1	3	
Reporting	2				1	1	
Obsolescence Management	3			1		2	
Training	3				1	2	
Subcontractor Flow Down	7			5		1	1
Customer Flow Down	0	1					
Mechanical Parts/Materials	6			4	2		
	57	2	1	19	10	22	5

Figure 8: Contractor Checklist Breakdown



Contractor Compliance Audit Checklist
(Counterfeit Parts and Materials)

Contractor:
Location:
Date:
Auditor(s):

Revision Date: May 1, 2015

0%

Item Designator	Counterfeit	Significance Factor	Contractor Compliance Rating	Score (Best Practices)
	Supplier Approval			0%
A1	Does the process for adding suppliers include appropriate supplier forms with specific reference to counterfeit avoidance and detection?	2		0.0
A2	Does the process for adding suppliers include verification of the supplier's selection and rating system to ensure the risk of low-quality or counterfeit parts is addressed?	3		0.0
A3	Does the process for adding suppliers include checking contractor history with the supplier, as well as checking government or commercial databases such as GIDEP and	5		0.0

Contractor Compliance Audit Checklist
Ratings Guidance

Revision Date: May 1, 2015

Item Designator	Counterfeit	Rating Guidance (0 to 5) 0	1	2	3
A2	Does the process for adding suppliers include verification of the supplier's selection and rating system to ensure the risk of low-quality or counterfeit parts is addressed?	No mention is made of a supplier ASL (Approved Supplier Listing).	Process confirms the supplier has a rating method for its suppliers.	Process confirms there is a rating method to at least the level of "approved" and "disapproved".	Process confirms the rating method which approved, disapprov provisional.
A3	Does the process for adding suppliers include checking contractor history with the supplier, as well as checking government or commercial databases such as GIDEP and ERAI?	No checking of contractor history is performed.	Only local contractor history is checked.	Local contractor history is checked, along with GIDEP history.	Local contractor hist along with GIDEP an history.

Figure 9: Sample Contractor Checklist Questions and Guidance

Appendix A: Critical Materiel Definitions

Reference	Definition
Critical Safety Item (CSI)	
DFARS, Subpart 209.270 SECNAVINST 5000.2E, DON Implementation and Operation of the DAS and JCIDS SECNAVINST 4140.2 Management of Aviation Critical Safety Items DODM 4140.01 – DOD Supply Chain Materiel Management Procedures, Volume 11	A part, an assembly, installation equipment, launch equipment, recovery equipment, or support equipment for a ship, aircraft, or weapon system if the part, assembly, or equipment contains a characteristic any failure, malfunction, or absence of which could cause (a) catastrophic or critical failure resulting in the loss of or serious damage to the ship, aircraft, or weapon system, (b) an unacceptable risk of personal injury or loss of life, or (c) an uncommanded engine shutdown that jeopardizes safety. A part, assembly, support equipment, installation, or production system containing a critical characteristic whose failure, malfunction, or absence may cause a catastrophic or critical failure resulting in loss or serious damage, unacceptable risk of personal injury or loss of life, or an unsafe condition.
Critical Application Item (CAI)	
SECNAVINST 4140.2 Management of Aviation Critical Safety Items	An item that is essential to weapon system performance or operation, or the preservation of life or safety of operating personnel, as determined by the military services. The subset of CAIs whose failure could have catastrophic or critical safety consequences (Category I or II as defined by MIL-STD-882) is called CSIs.
Information and Communications Technology (ICT) Components	
DODI 5200.44 - Protection of Mission Critical Functions to Achieve Trusted Systems and Networks	A component which is or contains information and communications technology (ICT), including hardware, software, and firmware, whether custom, commercial, or otherwise developed, and which delivers or protects mission critical functionality of a system or which, because of the system's design, may introduce vulnerability to the mission critical functions of an applicable system.
Controlled Inventory Item (CII)	
DODM 4140.01-V11 – DOD Supply Chain Materiel Management Procedures, Volume 11	Those items designated as having characteristics that require that they be identified, accounted for, secured, segregated, handled or transported in a special manner to ensure their integrity and that they are safeguarded. The list of CII codes includes NWRM, non-nuclear missiles and rockets, arms, ammunition, and explosives. CII categories in descending order of the degree of control normally exercised are classified items, sensitive items, and pilferable items.

This page intentionally left blank

Appendix B: Industry Standards

The following Industry Standards provide counterfeit avoidance and risk mitigation information. It is not an all-inclusive list. Use latest revisions of standards.

ANSI ESD S20.20 – "Development of an Electrostatic Discharge Control Program"

IDEA-ICE-3000 – "Professional Inspector Certification Exam"

IDEA-STD-1010 – "Acceptability of Electronic Components Distributed in the Open Market".

IPC J-STD-033 – "Handling, Packing, Shipping and Use of Moisture/Reflow Sensitive Surface Mount Devices"

ISO 17025 – "General Requirement for the Competence of Testing and Calibration Laboratories"

ISO 9001 – "Quality Management Systems – Requirements"

SAE ARP6178 – "Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors".

SAE ARP6328 – "Guideline for Development of Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Systems".

SAE AS5553 – "Counterfeit Electrical, Electronic, and Electromechanical (EEE) Parts; Avoidance, Detection, Mitigation, and Disposition"

SAE AS6081 – "Fraudulent/Counterfeit Electronic Parts: Detection, Mitigation, and Disposition – Distributors"

SAE AS6171 – "Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts"

SAE AS6174 – "Counterfeit Materiel: Assuring Acquisition of Authentic and Conforming Materiel"

SAE AS6301 – "Compliance Verification Criterion Standard for SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Detection, Mitigation, and Disposition – Distributors"

SAE AS6462 – "AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria"

SAE AS6496 – "Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition - Authorized/Franchised Distribution"

SAE AS6886 – “Counterfeit Materiel; Assuring Acquisition and Use of Authentic and Conforming Refrigerant”

SAE AS9100 – “Quality Management Systems - Requirements for Aviation, Space, and Defense Organizations”

SAE AS9120 – “Quality Management Systems – Requirements for Aviation, Space, and Defense Distributors”

Appendix C: Summary of Applicable DFARS Clauses

- DFARS 252.246-7007, Contractor Counterfeit Electronic Part Avoidance and Detection System.
  This clause adds the requirement for compliance (with the requirements for identifying, avoiding, and reporting counterfeit parts) to the existing requirements for the contractor's purchasing system. By adopting this approach, the Government's role in reviewing and monitoring the contractor's processes and procedures for detecting and avoiding counterfeit or suspect counterfeit electronic parts is addressed as part of a contractor's purchasing system review, to avoid creating a separate, new review requirement. This applies only to contractors (and their subcontractors) that are subject to the Cost Accounting Standards (CAS-covered).

- DFARS 252.246-7008, Sources of Electronic Parts.
  This clause applies for all electronic part procurements (including assemblies and commercial off the shelf assemblies), for all contractors and subcontractors, and establishes a clear priority in purchasing electronic parts from low risk suppliers.

- DFARS 231.205-71, Cost of remedy for use or inclusion of counterfeit electronic parts and suspect counterfeit electronic parts.
  This clause states that the costs of counterfeit electronic parts or suspect counterfeit electronic parts and the cost of rework or corrective action that may be required to remedy the use or inclusion of such parts are unallowable, along with the exceptions.

- DFARS 242.302, Contract Administration Functions.
  Clause (S-76) provides for review and audit of contractor-approved suppliers per 252.246-7008.

- DFARS 244.303, Extent of contractor purchasing systems reviews.
  This clause requires that the reviews of contractors' purchasing systems must include the adequacy of the contractor's counterfeit electronic part avoidance and detection system under DFARS 252.246-7007.

- DFARS subpart 246.870, Contractor Counterfeit Electronic Part Detection and Avoidance.
  A new policy on counterfeit parts has been added to DFARS subpart 246.8 which prescribes policy and procedures for preventing counterfeit parts when procuring electronic parts or end items, components, parts or materials that contain electronic parts. It provides minimum system criteria that a contractor's counterfeit electronic avoidance and detection system must address.

- DFARS 252.244-7001, Contractor Purchasing Administration.
  This clause was modified to include reference to DFARS 252.246-7007 for inclusion into the contractors purchasing system. It also contains the full text of Alternate Clause as required by DFARS 244.305-71.

- DFARS 244.305-71, Use of Contractor Purchasing System Administration clause.
  This clause states that clause 252.244-7001 (Contractor Purchasing System Administration—Alternate I) should be used in solicitations and contracts that contain the clause at 252.246-7007 (Contractor Counterfeit Electronic Part Detection and Avoidance System) but do not contain FAR 52.244-2 (Subcontracts).

Appendix D: Sample Statement of Work Language

The following provides information that should be considered for inclusion into the Statements of Work (SOW) for solicitations or contracts where counterfeit materiel is identified as a risk. These are only examples and can be used together or separately, and should be modified or otherwise tailored to meet program requirements:

D.1 Counterfeit Parts and Materials Planning

The contractor planning shall document procedures and processes to minimize the risk of procuring and/or using counterfeit parts and materials, and their process for detecting counterfeit materiel in the event it is procured. This requirement applies to both new/modified and existing mission and safety critical hardware. SAE AS5553 contains information regarding the detection, avoidance, and mitigation of counterfeit electronic components, and may be used as a reference document for the development of the plan.

D.2 Counterfeit Parts and Materials System

The Contractor's counterfeit electronic part avoidance and detection process shall implement policies and procedures that address:

- The training of personnel
- The inspection and testing of electronic parts
- Processes to abolish counterfeit parts proliferation
- Mechanisms to enable traceability of parts to suppliers
- Use and qualification of low risk suppliers
- The reporting and quarantining of counterfeit electronic parts and suspect counterfeit electronic parts
- Methodologies to identify suspect counterfeit parts and to rapidly determine if a suspect counterfeit part is, in fact, counterfeit
- The design, operation, and maintenance of systems to detect and avoid counterfeit electronic parts and suspect counterfeit electronic parts
- The flow down of counterfeit avoidance and detection requirements to subcontractors

D.3 Purchases from Unauthorized Suppliers

Parts and materials shall not be purchased from unauthorized suppliers (e.g. independent distributor or broker) unless there is no other means for procurement. In isolated cases when an unauthorized supplier is the only possible choice for procurement, an unauthorized supplier purchase report shall be provided to the program office. The report shall contain the following information:

- Reason why an authorized supplier or OM could not provide the part or material
- Product certificate of conformance with full supply chain traceability to the OM, if available
- Verification and authenticity data results (e.g., visual inspection, marking/surface finish permanency, DPA, Scanning Acoustic Microscopy, Energy Dispersive X-Ray Spectroscopy, Fourier Transform Infrared (FTIR) Spectroscopy, Rockwell Hardness Test, etc.)

Parts and materials that are part of commercial assemblies should also be procured only from OMs or authorized suppliers. For true commercial assemblies, built and provided unmodified to multiple customers, it may not be possible to enforce these requirements as strictly.

D.4 Preventing Counterfeit Parts and Materials

The contractor shall take steps as defined below to minimize the risk of receiving counterfeit parts and materials. The Contractor shall:

- Maximize availability of authentic, originally designed and/or qualified parts throughout the product's life cycle, including management of parts obsolescence
- Assess potential suppliers to minimize the risk of receiving counterfeit parts or materials
- Maintain a listing of approved suppliers with documented criteria for approval and removal of suppliers from the list
- Have purchasing procedures which require the selection of parts and materials from OM or authorized suppliers whenever possible
- Require a certificate of compliance and supply chain traceability for all electronic part purchases, and provide to the Government upon request
- Use Government or industry services such as GIDEP and other commercially available services to identify part or supplier quality or authenticity problems
- Define minimum inspection and test requirements for parts being procured from unauthorized suppliers, and shall ensure that in-house, third-party, and/or distributor inspection and test procedures and facilities comply with these requirements
- Incorporate procurement clauses which plainly identify quality requirements and liability to all approved suppliers
- Flow the requirements above to affected subcontractors

Parts and materials shall not be purchased from unauthorized sources (e.g. independent distributor or broker) unless there is no other means for procurement. In isolated cases when an unauthorized supplier is the only possible choice for procurement, an Unauthorized Supplier Purchase Report (CDRL XXXX) shall be provided to the contracting officer and program office. The report shall contain the following information:

- Reason why an authorized supplier or original component manufacturer (OM) could not provide the part or material
- Product certificate of conformance with traceability to the OM, if available
- Verification and authenticity data results (e.g., visual inspection, marking/surface finish permanency, DPA, Scanning Acoustic Microscopy, Energy Dispersive X-Ray Spectroscopy, Fourier Transform Infrared (FTIR) Spectroscopy, Rockwell Hardness Test, etc.)

SAE AS5553 contains information regarding the detection, avoidance, and mitigation of counterfeit electronic components, and may be used as a reference document for meeting the above steps.

D.5 Preventing Counterfeit Materiel

The Contractor shall implement steps as defined below to minimize the risk of receiving counterfeit materiel. The Contractor:

- Shall maximize availability of authentic, originally designed and/or qualified parts throughout the product's lifecycle, including management of parts obsolescence
- Shall assess potential suppliers to minimize the risk of receiving counterfeit materiel
- Shall maintain a listing of approved suppliers with documented criteria for approval and removal of suppliers from the list
- Shall have purchasing procedures which require the selection of parts and materiel from OM or authorized suppliers whenever possible
- Shall require a certificate of compliance and supply chain traceability for all materiel purchases
- Shall use Government or industry services such as Government-Industry Data Exchange Program (GIDEP) and other commercially available services to identify part or supplier quality or authenticity problems
- Shall define minimum inspection and test requirements for materiel being procured from unauthorized suppliers, and shall ensure that in-house, third-party, and/or distributor inspection and test procedures and facilities comply with these requirements
- Shall incorporate procurement clauses which plainly identify quality requirements and liability to all approved suppliers
- Shall flow the requirements above to affected Subcontractors

SAE AS6174 contains information regarding the detection, avoidance, and mitigation of counterfeit materiel, and may be used as a reference document for meeting the above steps.

D.6 Counterfeit Parts and Materials

The Contractor shall provide a Counterfeit Prevention Plan (CDRL XXXX) that documents procedures to minimize the risk of procuring and/or using counterfeit parts and materials. This plan shall be in accordance with DFARS 252.246-7007 Contractor Counterfeit Electronic Part Detention and Avoidance. Solicitations and subcontracts for all suppliers shall contain a requirement for procedures to minimize the risk of procuring and/or using counterfeit parts and materials.

D.6.1 Preventing Counterfeit Parts and Materials

The Contractor shall implement steps as defined in DFARS 252.246-7007 to minimize the risk of receiving counterfeit parts and materials. Parts and materials shall not be purchased from unauthorized suppliers (e.g. independent distributor or broker) unless there is no other means for procurement. In isolated cases when an unauthorized supplier is the only possible choice for procurement, a Technical Report – Study/Services, Unauthorized Supplier Purchase Report (CDRL XXXX) shall be provided to the contracting officer and the program office. The report shall contain the following information:

- Reason why an authorized supplier or OM could not provide the part or material
- Product certificate of conformance with traceability to the OM, if available
- Verification and authenticity data results (e.g., visual inspection, marking/surface finish permanency, Differential Power Analysis (DPA), Scanning Acoustic Microscopy, Energy

Dispersive X-Ray Spectroscopy, Fourier Transform Infrared (FTIR) Spectroscopy, Rockwell Hardness Test, etc.)

SAE AS5553 contains information regarding the detection, avoidance, and mitigation of counterfeit electronic components, and may be used as a reference document for meeting the above steps.

D.7 Counterfeit Parts and Materials

The following minimum processes shall be implemented and flowed down by the Contractor to all subcontractors In order to minimize the risk of use of counterfeit parts in *(NAME OF PROGRAM/EQUIPMENT)*, spare parts and associated equipment.

The contractor shall establish processes to minimize the risk of procuring and using counterfeit parts and materials. The contractor shall document these processes and provide those documented processes to Government representatives upon request.

At a minimum, these processes shall ensure that:

- All components for *(NAME OF PROGRAM/EQUIPMENT)* electronic assemblies and subassemblies are purchased from Original Manufacturer (OM), authorized suppliers, or franchised distributors; At a minimum, the contractor shall ensure that procurement practices and processes to purchase and install components from OM, authorized suppliers, or franchised distributors are flowed down to subcontractors and suppliers at all tiers
- A counterfeit Prevention Plan shall be generated in accordance with DI-MISC-81832 Counterfeit Prevention Plan, and that the requirements of this DID and AS5553 are flowed down to all subcontractors and suppliers in this effort;
- The Contractor shall maximize the use of authentic, originally designed and/or qualified parts
- The contractor shall assess potential suppliers to minimize the risk of receiving counterfeit parts or materials
- The contractor shall have purchasing procedures which confirm whether a selected supplier is authorized (as defined in SAE AS5553) for each purchase
- The contractor shall define minimum inspection and test requirements for parts being procured and shall ensure that in-house, third-party, and/or supplier inspection and test procedures and facilities comply with the requirements of this section. These minimum inspection and test requirements shall specify appropriate test methods to detect potential counterfeit parts and materials
- The contractor shall require a certificate of conformance (as defined in SAE AS5553) and supply chain traceability for all electronic part purchases
- The contractor shall use government or industry services such as GIDEP and other commercially available services to identify part or supplier quality or authenticity problems

The Contractor shall notify *(NAME OF PROGRAM OFFICE)* of the occurrence of a confirmed counterfeit part or material and the actions taken to identify, contain, and impound all product from the lot, within 7 working days of confirmation of the counterfeit status. The Contractor shall flow down a requirement for similar notification from Subcontractors or suppliers at any tier to the Contractor. The contractor shall initiate and submit an ALERT to the Government-Industry Data Exchange Program (GIDEP) within 60 days of knowledge of the counterfeit part or material.

Counterfeit parts are defined in SAE Aerospace Standard 5553. Counterfeit parts may be electronic or mechanical in nature. Counterfeit electronic parts may typically be used parts which have been refurbished and represented as new. Commonly counterfeited electronic parts include parts such as microcontrollers or specially screened devices, or common parts, which have several pin-compatible versions from multiple manufacturers, such as memory devices and operational amplifiers. Counterfeit mechanical parts are typically improperly made, marked, or treated products. Examples are improper anodization or heat treatments (or falsified data), mismarked parts sold as higher grade steel, or used/fake parts such as valves or circuit breakers.

D.8 Data Item Description

Data Item Description (DID) DI-MISC-81832, Counterfeit Prevention Plan: This DID describes the format and content of a contractors "Counterfeit Prevention Plan," and should be used by the procurement activity when requesting delivery of a counterfeit prevention plan.

D.9 Grey Market Statement (For CISCO Equipment)

Reseller and Equipment Qualification: Reseller shall certify that it is a CISCO Authorized Channel Partner as of the date of the submission of their offer, and that it has the certification/specialization level required by the Manufacturer to support both the product sale and product pricing, in accordance with the applicable Manufacturer certification/specialization requirements: Please provide proof of certification level with your quote submission. If proof of certification level is not provided with your quote submission, your quote may be considered non-responsive. Vendor shall warrant that the products are NEW and in their original UNOPENED box. Only CISCO installed and configured components are acceptable. Installation and / or configuration of third party components, or installation and / or configuration of OM components by any other than CISCO are NOT acceptable. The Vendor confirms to have sourced all Manufacturer products submitted in this offer from Manufacturer or through Manufacturer Authorized Channels only. Vendor shall provide Buyer with a copy of the End User license agreement pre-award, and shall certify that all Manufacturer software is licensed originally to Buyer as the original licensee authorized to use the Manufacturer Software. Only authentic OM equipment and support services sourced from authorized OM channels are acceptable. Equipment, materials, and services not meeting the above stated qualifications are not acceptable and will be returned to the reseller.

D.10 Containing Counterfeit Parts and Materials

Suspect counterfeit parts and materials shall be impounded with all other items from the same lot. The contractor shall identify and locate all potential users or hardware items with the suspect part or material, and contain product which has this suspect product, pending confirmation of the part or material's authenticity. The OM may be involved at this point in order to verify authenticity. Confirmed counterfeit material shall be contained and provided to investigative agencies for ongoing investigation or prosecution. The counterfeit product shall not be scrapped or otherwise disposed of without approval from investigative authorities or the program office. Confirmed counterfeit product shall not be returned or handled in a way which would allow its resale or reuse. Suspect counterfeit parts or materials whose authenticity (or lack of) cannot be definitively determined, shall be dispositioned via Material Review Board (MRB).

D.11 Reporting Counterfeit Parts and Materials

The prime contractor and program office shall be notified of the occurrence of a suspect or confirmed counterfeit part or material, and the actions taken to identify, contain, and impound all product from the lot. The contractor shall also contact the OM, and supplier if applicable. The contractor shall initiate and submit an ALERT to the Government-Industry Data Exchange Program (GIDEP) within 60 days of knowledge of the counterfeit part or material. The contractor shall notify the appropriate parties to document the case for legal action if required (e.g., contracting officer, DOD Office of Inspector General).

D.12 Nonconforming Material and Parts

Electrical components which fail during production or acceptance testing shall be assessed to determine if the supplier of the part was an authorized supplier for the manufacturer. Analysis of these failures shall include assessment of part authenticity (potential of being counterfeit or fraudulent).

D.13 Warranty "Counterfeit"

D.13.1 Seller warrants the goods delivered pursuant to this Contract, unless specifically stated otherwise in this Contract, shall (i) be new (ii) be free from defects in workmanship, materials, and design and (iii) be in accordance with all the requirements of this Contract. Seller further warrants that the performance of work and services shall conform with the requirements of this Contract and to high professional standards. All warranties in this Contract shall survive inspection, test, final acceptance and payment of goods and services.

D.13.2 Unless Buyer expressly identifies the goods that are procured under this Contract as non-technical and for Buyer's internal use only, Seller warrants without limitation as to time that the goods delivered pursuant to this Contract shall (i) be and only contain materials obtained directly from the OM or an authorized OM reseller or distributor (collectively, an Authorized Distributor); (ii) not be or contain Counterfeit Items or Suspect Counterfeit Items, as defined below; and (iii) contain only authentic, unaltered OM labels and other markings. Seller shall obtain and retain all documentation required to fully trace the distribution and sale of the goods delivered hereunder back to the relevant OM, and, on request of Buyer, shall provide such authenticating documentation. Counterfeit Item means an unlawful or unauthorized reproduction, substitution, alteration, or the false identification of grade, serial number, lot number, date code, or performance characteristic, that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified item from the OM, an Authorized Distributor, or an Aftermarket Manufacturer as defined in SAE AS5553 "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition" (Authorized Aftermarket Manufacturer). A Suspect Counterfeit Item means an item for which credible evidence (including, but not limited to, visual inspection or testing) provides reasonable doubt that the item is authentic. Seller warrants that it will not act as or engage an independent distributor, non-authorized distributor, non-franchised distributor, non-authorized supplier, or non-authorized reseller (collectively, Broker), to assist it in delivering goods pursuant to this Contract unless the Buyer provides prior written approval to do so. Any Seller request to procure from a Broker shall include complete and compelling support for such request and shall include all actions completed by Seller to ensure the goods thus procured are not Counterfeit Items. Seller's supporting documentation shall include: (i) results of authentication test and analysis conducted (reference SAE AS5553), (ii) traceability with identification of all supply chain intermediaries wherever such traceability

exists, and (iii) identification of and traceability to the source for any remarked or resurfaced material. Seller shall include the substance of this Section in any agreement between Seller and Seller's lower tier subcontractors, including in any agreement between Seller and Seller's Broker, and Seller shall cause Seller's lower tier subcontractors and Seller's Broker to include the substance of this Section in all agreements with any of their lower tier subcontractors.

D.13.3 Unless Buyer expressly identifies the goods that are procured under this Contract as non-technical and for Buyer's internal use only, Seller, as OM, Authorized Distributor, Authorized Aftermarket Manufacturer, or Broker approved by Buyer, further warrants that it has and shall maintain a Counterfeit Item risk mitigation process, internally and with its suppliers, (reference SAE AS5553), for goods delivered hereunder, and in accordance with the standards or instructions set forth in any Buyer's specifications and other required provisions and specifications incorporated into this Contract. Buyer shall have the right to audit, inspect, and / or approve the processes at any time before or after delivery of the goods ordered hereunder. Seller shall provide evidence of the Seller's risk mitigation process to Buyer upon request. Buyer shall have the right to require changes to the processes to conform with Buyer's defined standards, if any. Seller and Seller's lower-tier subcontractors that are allowed access to the US Government Industry Data Exchange Program (GIDEP) shall participate in monitoring GIDEP reports and Seller shall act on GIDEP reports that affect product delivered to Buyer. Seller shall immediately notify Buyer with the pertinent facts if Seller becomes aware of or suspects that items delivered for the Contract are, or contain, suspect or confirmed counterfeit items. Failure of the Seller or any of its lower-tier subcontractors to conform its processes with Buyer's defined standards may result in the termination of this Contract in accordance with the termination provisions set forth herein. If, during Buyer's inspection procedures, a good delivered hereunder is discovered to be a Counterfeit Item or Suspect Counterfeit Item, Buyer shall have the right to quarantine the good for further investigation of its authenticity. Buyer's investigation may include the participation of third parties or governmental investigative agencies as required by law or regulations by Buyer's customer, or by Buyer, in its sole discretion. The Seller and/or the Seller's lower-tier subcontractors shall cooperate in good faith with any investigation conducted by Buyer, including, but not limited to, cooperation by Seller's or Seller's lower-tier subcontractor's staffs responsible for the maintenance and disclosure of all design, development, manufacturing, and traceability records with respect to the good in possession of Seller or Seller's lower-tier subcontractor. Upon Buyer's request, Seller shall provide Buyer certificates of conformance with respect to the goods delivered. Buyer shall not be required to return the good to the Seller during the investigation process or thereafter. Buyer shall not be liable for payment to Seller of the price of any Suspect Counterfeit Items under investigation. When so authorized by Buyer, Seller shall be responsible for counterfeit risk mitigation testing and providing traceability identifiers (i.e. Date Code / Lot Code, Serial number) for Broker procured parts, and identifying items delivered to Buyer that contain such parts. If Buyer determines in its sole discretion that there is credible evidence after visual inspection, testing, or other information that a good delivered under this Contract may have been misrepresented by the Seller or Seller's lower-tier subcontractor and constitutes a Counterfeit Item or Suspect Counterfeit Item, Seller, or its lower-tier subcontractor, shall, if directed by Buyer to do so, issue a GIDEP alert and shall ensure suspect or confirmed Counterfeit Items are not delivered to Buyer. Buyer reserves its right hereunder, to issue its own GIDEP alert if, after investigation, Buyer concludes, in its sole estimation, that a good is a Counterfeit Item or Suspect Counterfeit Item. Seller shall include the substance of this Section in any agreement between Seller and Seller's lower tier subcontractors, including in any agreement between Seller and Seller's Broker, and Seller shall cause Seller's lower tier subcontractors and

Seller's Broker to include the substance of this Section in all agreements with any of their lower tier subcontractors.

D.13.4 Seller warrants without limitation as to time that any hardware, software and firmware goods delivered under this Contract: (i) shall not contain any viruses, malicious code, Trojan horse, worm, time bomb, self-help code, back door, or other software code or routine designed to: (a) damage, destroy or alter any software or hardware; (b) reveal, damage, destroy, or alter any data.

D.14 Counterfeit Mitigation

Seller warrants that the goods delivered pursuant to this Contract shall (i) be and only contain materiels obtained directly from the OM or an authorized OM reseller or distributor; (ii) not be or contain Counterfeit Items, as defined below; and (iii) contain only authentic, unaltered OM labels and other markings. Seller shall obtain and retain all documentation required to fully trace the distribution and sale of the goods delivered hereunder back to the relevant OM, and, on request of Buyer, shall provide such authenticating documentation. Counterfeit Items include, but are not limited to, goods or separately-identifiable items or components of goods that: (i) are an illegal or unauthorized copy or substitute of an OM item; (ii) are not traceable to an OM sufficient to ensure authenticity in OM design and manufacture; (iii) do not contain proper external or internal materials or components required by the OM or are not constructed in accordance with OM design; (iv) have been re-worked, re-marked, re-labeled, repaired, refurbished, or otherwise modified from OM design but not disclosed as such or are represented as OM authentic or new; (v) have not passed successfully all OM required testing, verification, screening, and quality control processes; or (vi) an item with altered or disguised documentation, package labeling, or item marking intended to mislead a person into believing a non-OM item is genuine, or that an item is of better or different performance when it is not. Seller further warrants that it has and shall have an internal Counterfeit Item control process for goods delivered hereunder in accordance with the standards or instructions set forth in any Buyer's specifications, including but not limited to specifications, or other provisions incorporated into this Contract. Buyer shall have the right to audit, inspect, and / or approve the processes at any time before or after delivery of the goods ordered hereunder. Buyer shall have the right to require changes to the processes to conform to Buyer's defined standards, if any. Failure of the Seller to conform its processes to Buyer's defined standards may result in the termination of this Contract in accordance with the termination provisions set forth herein. Seller shall include this clause in any agreement between Seller and its lower tier sellers.

D.14.1 Seller warrants that any hardware, software and firmware goods delivered under this Contract: (i) shall not contain any viruses, malicious code, Trojan horse, worm, time bomb, self-help code, back door, or other software code or routine designed to: (a) damage, destroy or alter any software or hardware; (b) reveal, damage, destroy, or alter any data; (c) disable any computer program automatically; or (d) permit unauthorized access to any software or hardware; (ii) shall not contain any third party software (including software that may be considered free software or open source software) that (a) may require any software to be published, accessed or otherwise made available without the consent of Buyer, or (b) may require distribution, copying or modification of any software free of charge; and (iii) shall not infringe any patent, copyright, trademark, or other proprietary right of any third party or misappropriate any trade secret of any third party.

D.15 New Materiels; Anti-Counterfeit Mitigation

D.15.1 For Subcontractors, Contract Manufacturers, and Authorized Distributors - Only new and authentic materiel are to be used in products delivered to Buyer. No counterfeit or suspect counterfeit materiel is to be contained within the delivered product. Materiel shall be purchased directly from the OMs, or through the OMs Authorized Distributor. Documentation must be available that authenticates traceability to the applicable OM. Independent Distributors (Brokers) shall not be used without written consent from Buyer.

D.15.2 For Independent Distributors - Independent Distributor's procedures shall meet the intent of the requirements of IDEA-STD-1010 & SAE AS6081 and have a Quality Management System certified to AS9100 and/or AS9120. When available, the OM's Certificate of Conformance and all traceability documentation shall be included with each shipment of parts. It shall include the manufacturer's name, part number, date codes, lot codes, serializations, and / or any other batch identifications. Inspections and tests required are as noted in the Subcontract. Recorded evidence of all testing performed shall be included with each shipment. If suspect/counterfeit parts are furnished under this Subcontract and are found in any of the Goods delivered hereunder, such items will be impounded by Buyer. The Seller shall promptly replace such suspect/counterfeit parts with parts acceptable to the Buyer and the Seller shall be liable for all costs relating to the removal and replacement of said parts as specified in the Subcontract requirements or Distributor's insurance policies. Buyer reserves all contractual rights and remedies to address grievances and detrimental impacts caused by suspect/counterfeit parts.

D.16 Goods Warranty; Anti-Counterfeit Mitigation

D16.1 Seller warrants the Goods delivered pursuant to this Contract, unless specifically stated otherwise in this Contract, shall (i) be new; (ii) be and only contain materials obtained directly from the OM or an authorized OM reseller or distributor (Note - Independent Distributors (Brokers) shall not be used by Seller without written consent from Buyer); (iii) not be or contain Counterfeit Items; (iv) contain only authentic, unaltered OM labels and other markings; (v) have documentation made available upon request that authenticates traceability to the applicable OM; and (vi) be free from defects in workmanship, materials, and design and conform to all the specifications and requirements of this Subcontract. These warranties shall survive inspection, test, final acceptance and payment of Goods and Services.

D16.2 For purposes of this section, a "Counterfeit Item" is defined to include, but is not limited to, (i) an item that is an illegal or unauthorized copy or substitute of an OM item; (ii) an item that does not contain the proper external or internal materials or components required by the OM or that is not constructed in accordance with OM specification; (iii) an item or component thereof that is used, refurbished or reclaimed but the Seller represents as being a new item; (iv) an item that has not successfully passed all OM required testing, verification, screening and quality control but that Seller represents as having met or passed such requirements; (v) an item with a label or other marking intended, or reasonably likely, to mislead a reasonable person into believing a non-OM item is a genuine OM item when it is not or (vi) material that has been confirmed to be a copy, imitation or substitute that has been represented, identified or marked as genuine, and/or altered by a source without legal right with intent to mislead, deceive or defraud.

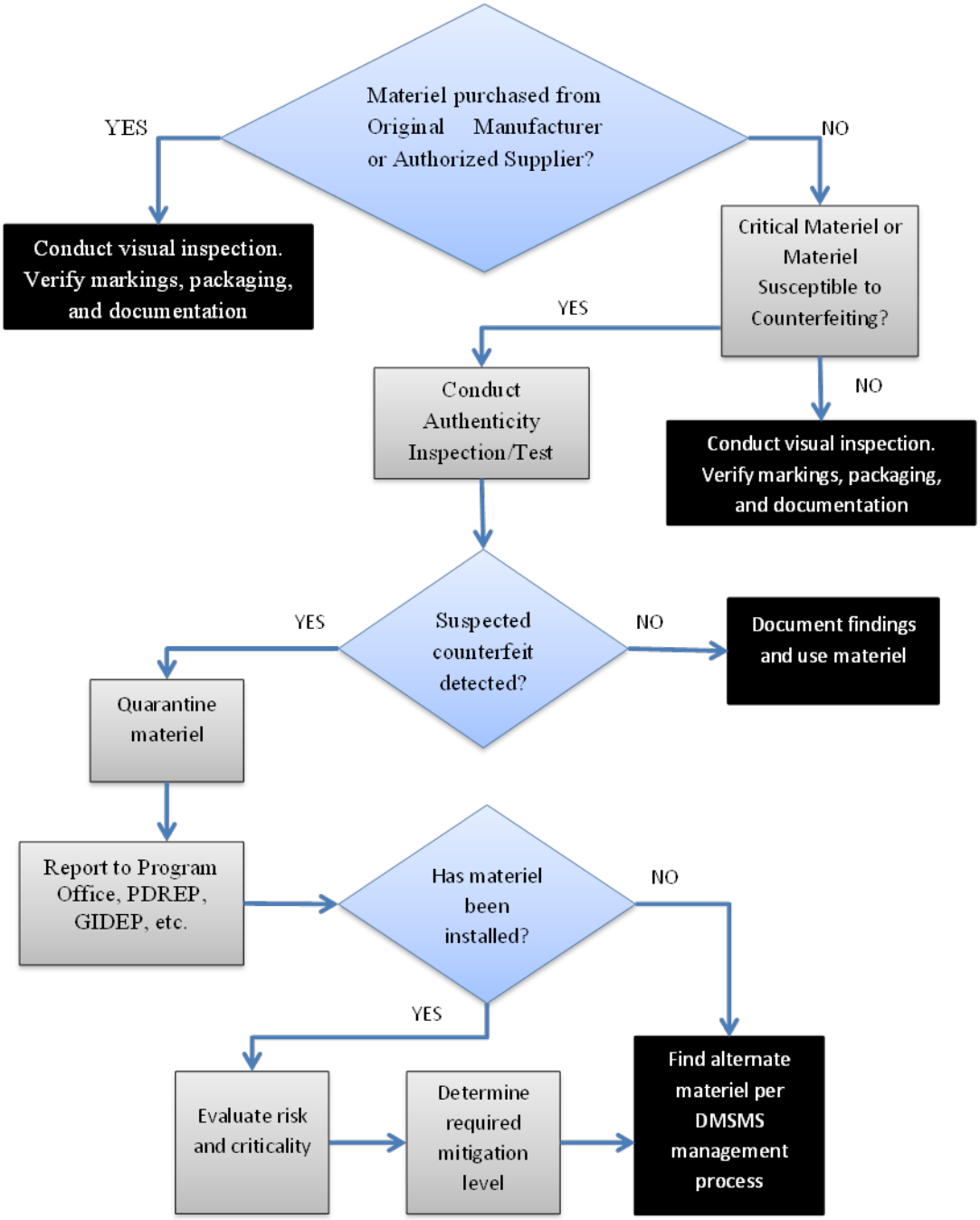
D16.3 Seller warrants that any hardware, software, and firmware Goods delivered under this Subcontract to the extent reasonably possible: (i) do not contain any viruses, malicious code, Trojan horse, worm, time bomb, self-help code, back door, or other software code or routine

designed to (a) damage, destroy, or alter any software or hardware; (b) reveal, damage, destroy, or alter any data; (c) disable any computer program automatically; or (d) permit unauthorized access to any software or hardware; and (ii) do not contain any 3rd party software (including software that may be considered free software or open source software) that (a) may require any software to be published, accessed or otherwise made available without the consent of Buyer or (b) may require distribution, copying or modification of any software free of charge;

D16.4 This warranty entitlement shall inure to the benefit of both Buyer and Buyer's customer and shall cover a period 12 months following final acceptance; and,

D16.5 Seller shall be liable for and save Buyer harmless from any loss, damage, or expense whatsoever that Buyer may suffer from the breach of any of these warranties. Remedies shall be at Buyer's election.

Appendix E: Suggested Authentication Process Flow



This page intentionally left blank

Appendix F: Indicators of Counterfeit Electronic Parts

The following table contains an overview of possible indicators that may point to a part being suspect counterfeit. While many of these indicators apply only to electronic parts, some would apply equally to all materiel (package inspection, documentation inspection, marking inspection, physical dimensions). No one indicator may be sufficient for classifying a part as suspect counterfeit. It is best practice to look for multiple indicators of counterfeiting. It is best to consider both the quantity and strength of indicators found to make a determination that a part is suspect counterfeit. Input from the original component manufacturer should weigh heavily in this determination if their input is available. This list is not an exhaustive list of applicable indicators or test types.

Test Type	Counterfeit Indicator	Strength of Indicator
External Package Inspection	Shipping damage to external packaging	Minor
	Misspelled wording on external packaging	Minor
	Wrong part number on external packaging	Moderate
	Erroneous OM Logo on external packaging	Major
Internal Package Inspection	Shipping damage to box/tube/tray/reel	Minor
	Misspelled wording on box/tube/tray/reel	Minor
	Wrong part number on box/tube/tray/reel	Moderate
	Wrong quantity notes on box/tube/tray/reel	Minor
	Bar code mismatch (scan vs human) on box/tube/tray/reel	Major
	Erroneous OM Logo on box/tube/tray/reel	Major
	Not in original manufacturer's packaging	Minor
	Use of non-ESD protected material	Moderate
	Not in a sealed moisture barrier bag	Minor
	Humidity indicator card (HIC does not change with humidity)	Major
	Wrong/inconsistent orientation in tube/tray/reel	Moderate
	Inconsistent design of tubes/trays/reels	Moderate
	Incorrect size for tube/tray	Moderate
Documentation Inspection	Misspelled wording in documentation	Minor
	Mismatch in part number or lot/DC in documentation	Moderate
	Mismatch in part quantity in documentation	Minor
	Erroneous OM Logo on documents	Major
	Evidence of tampering in documentation	Moderate
Part Marking / ID Inspection	Three or more date codes or lots in the same box/tube/tray/reel	Moderate
	Marking on part does not match documentation or packaging	Moderate
	Lot/DC on part does not match documentation or packaging	Moderate
	Impossible lot/DC on part or packaging (obsolete)	Major
	Inconsistent part indentation (pin 1, etc.), top or bottom	Major
	Inconsistent country of origin information	Major

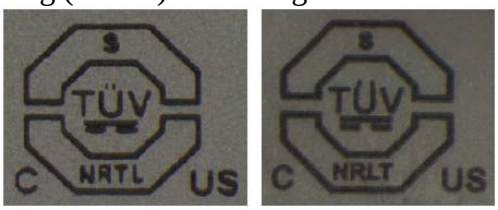
Test Type	Counterfeit Indicator	Strength of Indicator
	Incorrect/erroneous manufacturer logo	Major
	Texture within part indentations	Minor
	Misaligned markings on parts	Minor
	Inconsistent laser etch depth/width	Minor
	Part markings are poor quality	Minor
Physical Dimensions	Package dimensions fail specifications	Major
	Pin count is incorrect	Major
Part Surface Inspection	Superficial scratches or chips on part	Minor
	Major mechanical damage (chips, scratches, etc.)	Moderate
	Heat stress (bulges or blisters) on part	Major
	"Ghosted" markings visible on part surface	Major
	Sanding visible across part surface	Major
	Inconsistent texture or color on parts in same lot/DC	Moderate
	Suspicious texture or color on part	Minor
	Suspicious laser markings	Minor
	Internal die or wirebonds exposed to surface of part	Major
	Evidence of microblasting	Major
	Evidence of flat lapping	Major
	Chemical residue or other contamination on part	Minor
Lead / Solder Ball Inspection	Bent leads on part	Minor
	Replated part leads (no tooling marks)	Major
	Deformed leads/balls	Minor
	Wrong solder ball size	Moderate
	No exposed copper on end of leads	Minor
	Oxidized/corroded leads/balls	Minor
	Excessive scratches or scrapes on leads	Moderate
	Missing leads/balls	Moderate
	Solder splash on leads/balls	Moderate
	Evidence of microblasting	Moderate
	Reattached leads on part	Major
	Lead design varies on parts in same lot/DC	Moderate
Marking Permanency	Ink marking is removed by MS/alcohol	Moderate
	Surface coating is removed by MS/alcohol	Major
	Hidden "ghosted" markings uncovered by MS/alcohol	Major
	Internal die or wirebonds exposed by MS/alcohol	Major
	Sanding underneath surface uncovered by MS/alcohol	Major
Surface Scrape	Surface coating is removed by a razor knife	Major
	Sanding underneath surface exposed by razor knife	Major
Surface Finish Permanency	Ink marking is removed by acetone	Minor
	Surface coating is removed by acetone	Major
	Hidden "ghosted" markings uncovered by acetone	Major
	Internal die or wirebonds exposed by acetone	Major

Test Type	Counterfeit Indicator	Strength of Indicator
	Sanding underneath surface uncovered by acetone	Major
	Surface coating is removed by aggressive solvents	Major
	Hidden "ghosted" markings uncovered by aggressive solvents	Major
	Internal die or wirebonds exposed by aggressive solvents	Major
	Sanding underneath surface uncovered by aggressive solvents	Major
X-Ray Fluorescence	Inconsistent lead plating composition	Minor
	Incorrect lead plating composition	Moderate
Radiological (X-Ray)	Inconsistent die size or design on parts in same lot/DC	Major
	Misaligned die	Minor
	Cracked or damaged die	Major
	Inconsistent lead frame size or design on parts in same lot/DC	Major
	Damaged or deformed lead frame	Major
	Inconsistent wire bond thickness on parts in same lot/DC	Minor
	Inconsistent wire bond placement on parts in same lot/DC	Major
	Incorrect wire bond materiel	Major
	Missing wire bonds	Major
	Double ball bonds	Major
	Inconsistent die/lead frame thickness on parts in same lot/DC	Minor
Scanning Acoustic Microscopy	Hidden "ghosted" markings visible by shallow scan	Major
	Die delamination visible with CSAM scan	Minor
	Inconsistent die size or design on parts in same lot/DC	Major
	Inconsistent lead frame size or design on parts in same lot/DC	Major
Decapsulation	Inconsistent die size or design on parts in same lot/DC	Major
	Misaligned die	Minor
	Cracked or damaged die	Major
	Poor quality (e.g., traces, spacing, contamination, etc.)	Minor
	Wrong OM or logo	Major
	Mismatched part number	Minor
	Incorrect wire bond materiel	Major
	Inconsistent OM or logo on parts in same lot/DC	Major
	Inconsistent part number on parts in same lot/DC	Major
	Inconsistent die design on parts in same lot/DC	Major
	Inconsistent lead frame design on parts in same lot/DC	Major
	Impossible date code (die year after part DC)	Major
	Part is more difficult to decap compared to known good	Minor
Electrical Test	One-time programmable parts can't be programmed	Major
	Code/programming left over in parts	Major
	25% or higher electrical failure rate	Moderate
	10% or higher electrical failure rate	Minor
	5% or higher electrical failure rate	Minor

Test Type	Counterfeit Indicator	Strength of Indicator
	Electrical failures are gross (wrong/damaged)	Major
	Electrical failures are marginal (stress)	Minor
	Non-traditional electrical test variation	Minor
Known Good Part Comparison	Unmatched pin 1 indicator	Moderate
	Unmatched dimple placement	Moderate
	Unmatched font or lot format	Moderate
	Unmatched lead design	Moderate
	Unmatched lead frame	Minor
	Unmatched die markings	Minor
OM Support	Component manufacturer states parts are likely counterfeit	Major
	Component manufacturer states parts are possibly counterfeit	Moderate

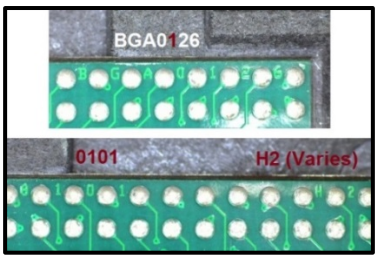
Appendix G: Examples of Counterfeit Electronic Parts

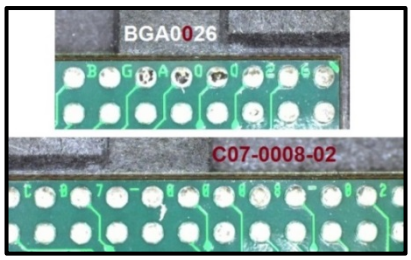
- Visual inspection revealed incorrect and misspelled logo. The phrase 'NRTL' denotes Nationally Recognized Test Laboratories, a listing of labs certified to certain test standards. The presence of a misspelling (NRLT) is a strong indicator that the label is counterfeit.

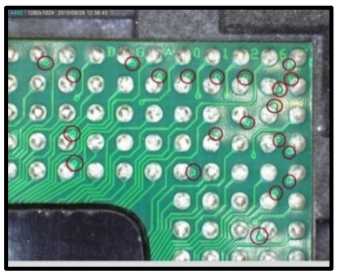


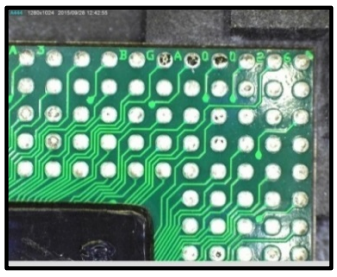
- Visual inspection revealed font inconsistencies.

- Visual inspection reveals variation in substrate design. This is highly unusual for parts from the same lot and date code.

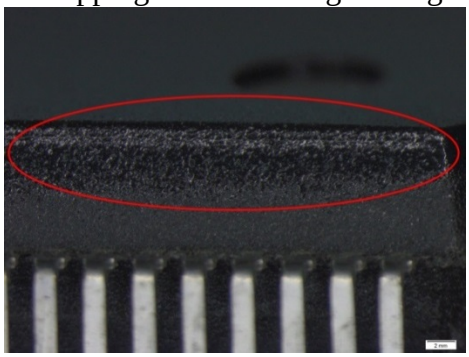




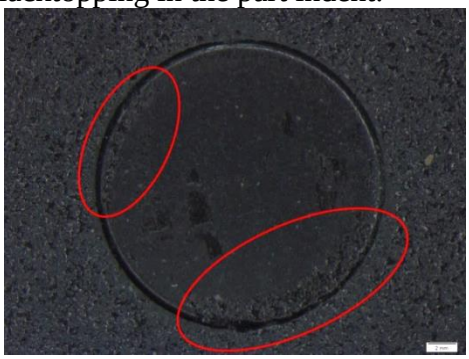




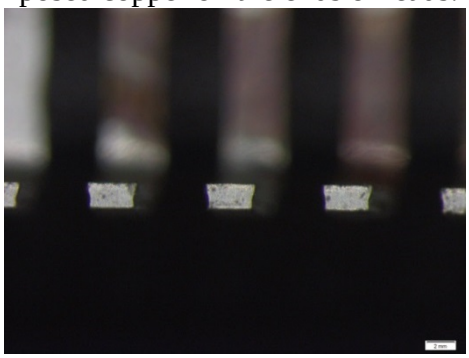
- Visual inspection revealed blacktopping material along the edge of the part.



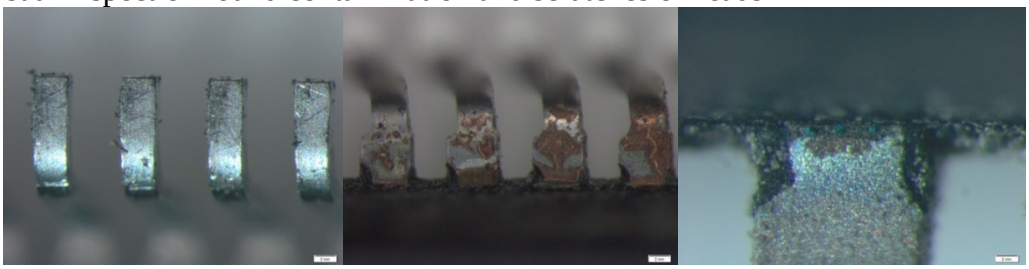
- Visual inspection revealed blacktopping in the part indent.



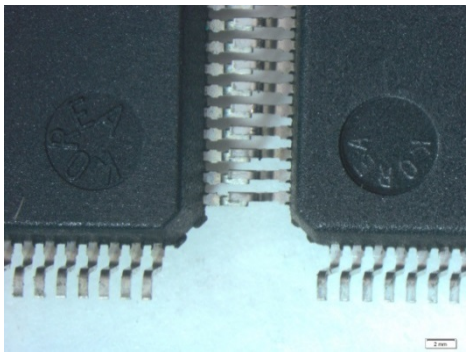
- Visual inspection found no exposed copper on the ends of leads.



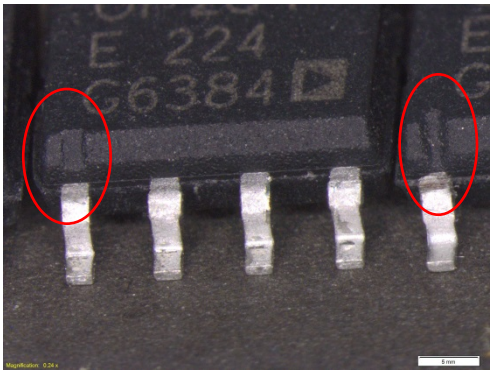
- Visual inspection found contamination and scratches on leads



- Visual inspection found different fonts for the country of origin. This is highly unusual for parts from the same lot and date code.

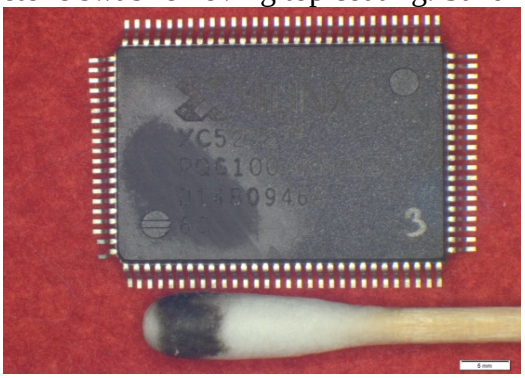


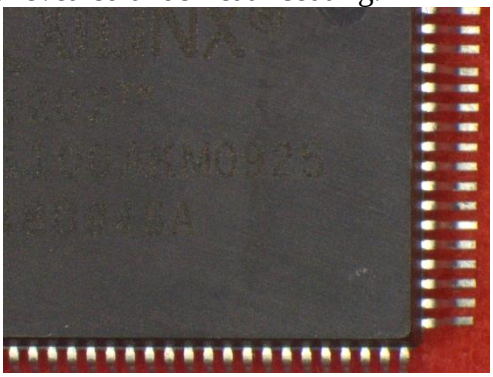
- Visual inspection found different Pin 1 indicators. This is highly unusual for parts from the same lot and date code.



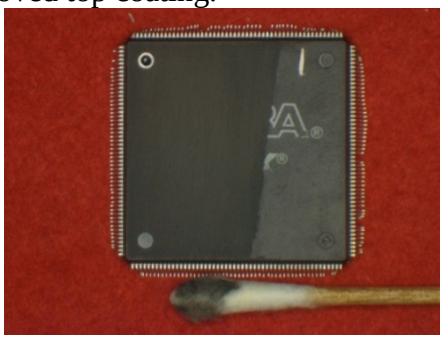
- Visual inspection found bent leads and major chip outs from part

- Acetone swab removing top coating. Sanding marks revealed underneath coating.

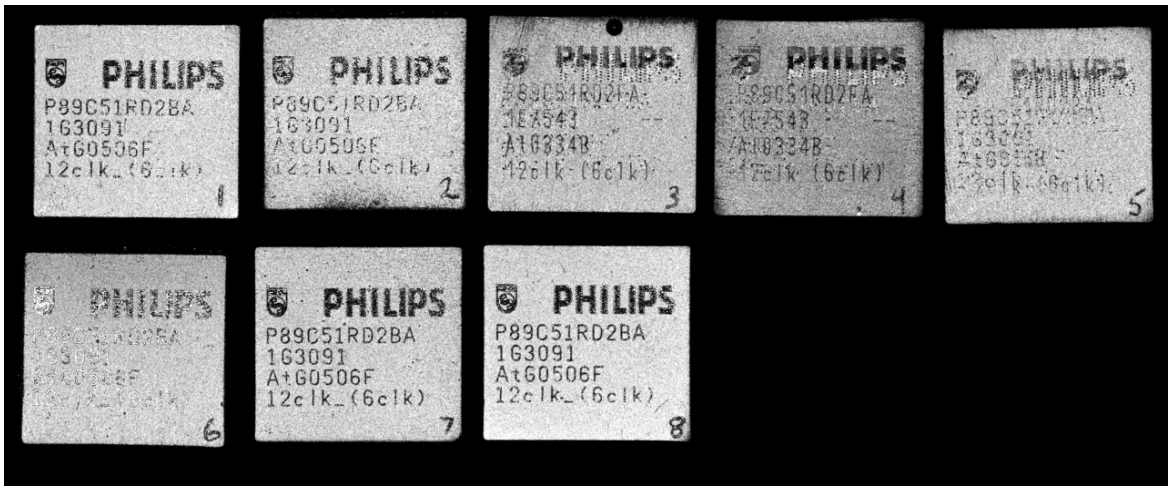




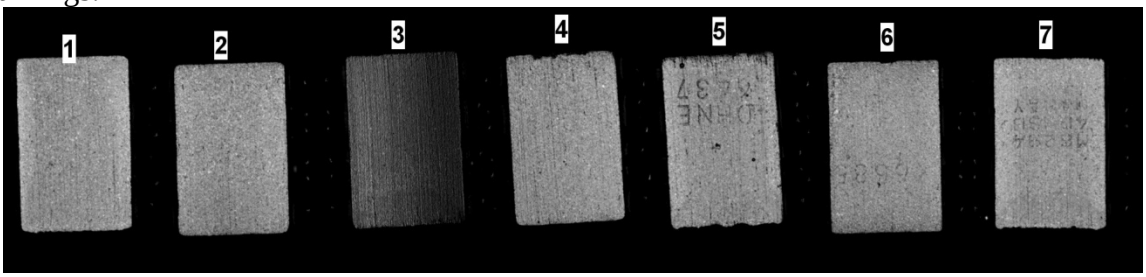
- DynaSolve 750 Solvents removed top coating.



- Visual inspection found suspicious laser markings. Acoustic microscopy found ghosted markings confirming the parts had been remarked

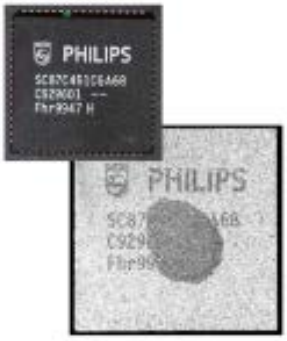


- Acoustic microscopy showed horizontal scratches indicative of sanding as well as ghosted markings.

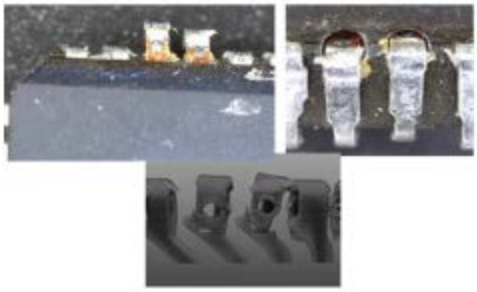


- Acoustic microscopy revealed ghosted markings. The devices were remarked as different speeds or different temperature ranges.

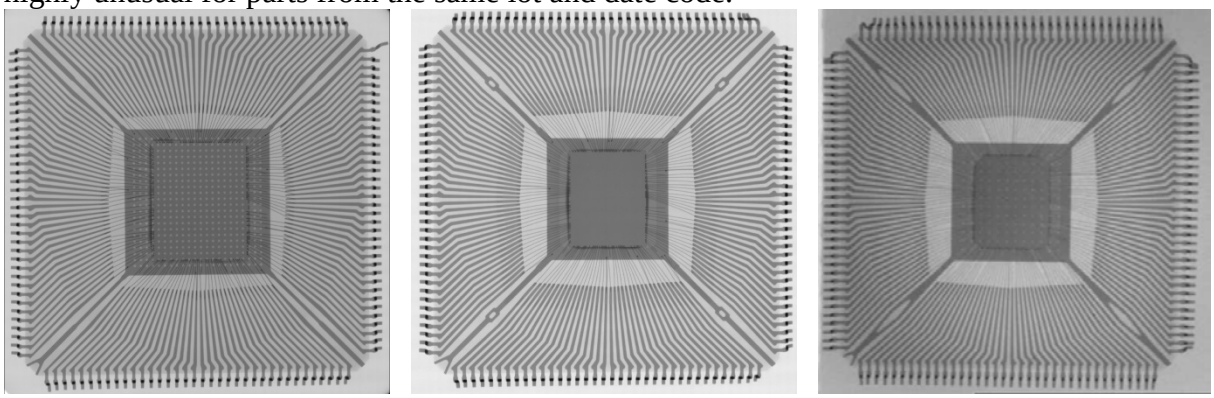
- Acoustic microscopy identified the center of the part contained a different material that was otherwise undetectable upon visual inspection.



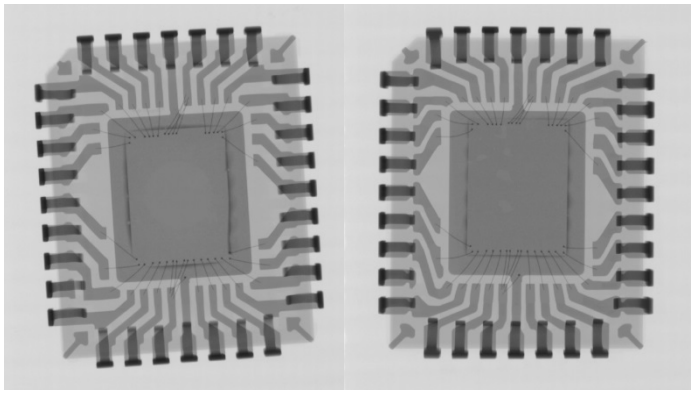
- Visual and X-Ray inspection revealed part with leads that were reattached.



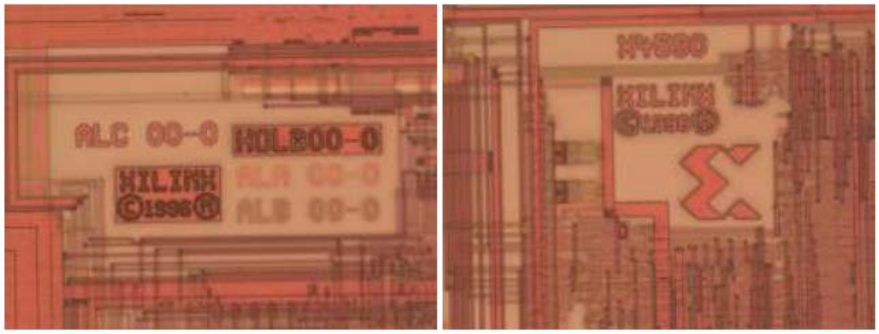
- X-Ray inspection found three different lead frame designs and two different die sizes. This is highly unusual for parts from the same lot and date code.

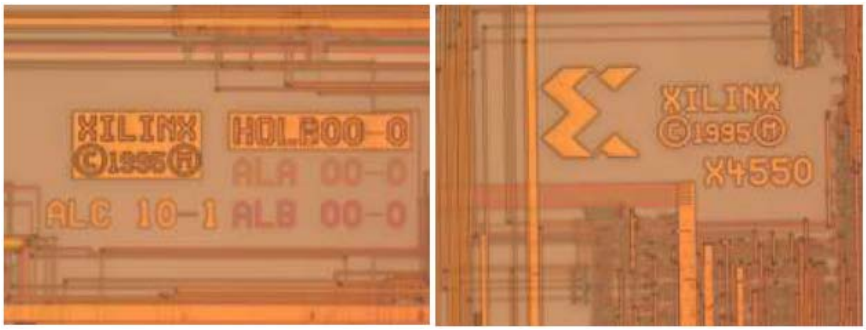


- X-Ray inspection found two different lead frame designs. This is highly unusual for parts from the same lot and date code.

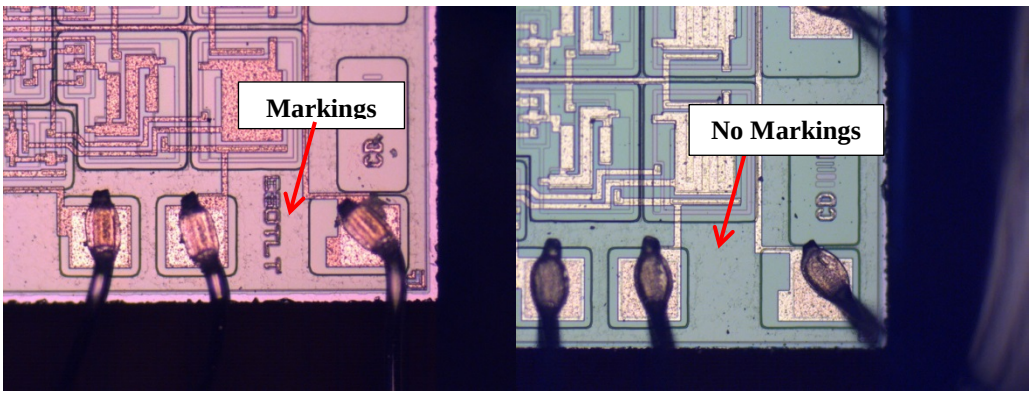


- Decapsulation revealed different die sizes as well as die markings. This is highly unusual for parts from the same lot and date code.





- Decapsulation revealed different die markings. This is highly unusual for parts from the same lot and date code.



Appendix H: Indicators of Counterfeit Mechanical Parts and Materials

Test/Materiel Type	Counterfeit Indicator	Strength of Indicator
Packaging Indicators	Inconsistent vendor name on the item and on the shipping container, or no name on the container	Moderate
	Shipping boxes contain mixed batch numbers, expiration dates, and UPC codes	Minor
	Unusual packaging and boxing of items	Moderate
	Inconsistent with the manufacturer's normal packaging or documentation requirements	Major
	Questionable or meaningless numbers on the item(s) or packaging	Moderate
	Obviously changed labeling (crossed out or erased)	Moderate
	Erroneous OM Logo on external packaging	Major
Nameplate Indicators	Appear to have been altered, photocopied, or painted over	Major
	Have incomplete or missing data	Moderate
	Preprinted labels that show typed entries	Moderate
	Attached in a different location than normal or with inconsistent fasteners (screws instead of rivets, or a combination of rivets and screws)	Moderate
	Missing manufacturer's standard markings, stamps, or logos, and with irregular stamping or inconsistent font Multiple logos and seals	Major
	Warning labels with grammatical errors or that conflict with information found elsewhere on the packaging	Major
	Obviously changed labeling (crossed out or erased)	Major
Documentation Indicators	Excessively faded or unclear or missing data	Moderate
	Use of correction fluid or correction tape	Major
	Type style, size, or pitch change is evident	Moderate
	Data on a single line is located at different heights	Moderate
	Lines on forms are bent, broken, or interrupted indicating data has been deleted or exchanged by "cut and paste"	Major
	Handwritten entries are on the same document where there is typed or preprinted data	Moderate
	Text on page ends abruptly and the number of pages conflicts with the transmittal	Moderate
	Corrections are not properly lined-out, initialed and dated	Moderate
	Document is not signed or initialed when required	Moderate
	The name of the document approver, or title, cannot be determined	Moderate
	Document has missing or illegible signature, initials	Moderate
	The name of the document approver, or title, cannot be determined	Major
	Approvers name and signature do not match	Major

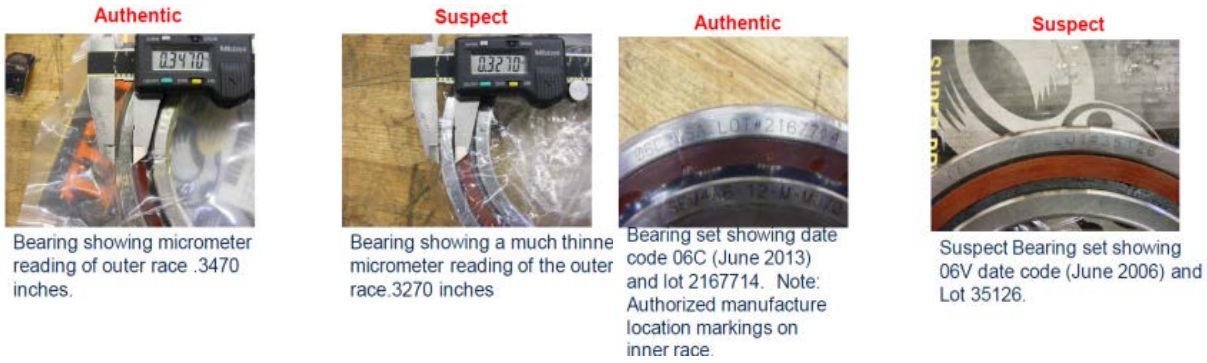
Test/Materiel Type	Counterfeit Indicator	Strength of Indicator
	Technical data is inconsistent with code or standard requirements	Major
	Certification/test results are identical between all tested item, expect normal variations	Moderate
	Documentation Certificate of Conformance and Testing is not delivered as required on the purchase order, or is in an unusual format	Moderate
	Document is not traceable to the items procured	Major
Miscellaneous Mechanical (Fasteners, Pipes, Fittings, etc.)	Pitting or corrosion	Moderate
	External weld or heat indications	Major
	Questionable or meaningless numbers	Major
	Typed labels	Moderate
	Evidence of hand-made parts	Major
	Painted stainless steel	Moderate
	Ferrous metals that are clean and bright	Moderate
	Excess wire brushing or painting	Minor
	Ground off casting marks or logos	Major
	Weld repairs	Major
	Threads showing evidence of wear or dressing	Moderate
	Inconsistency between labels	Moderate
	Old or worn nameplates	Moderate
	Missing manufacturer's standard markings and logos	Major
	Overlapping stamps	Moderate
	Different colors of the same part	Moderate
	Traces of Prussian Blue or other lapping compound	Moderate
	Used component appearance	Moderate
	Wrench marks	Moderate
	Scratches on component outer surface	Minor
	Missing markings	Moderate
	Missing ratings	Moderate
	Evidence of re-stamping	Major
	Wrong material	Major
	Deficient welds	Major
	Outside of dimensional specifications	Major
	Wrong country of origin	Major
	Wrong fasteners for nameplates	Moderate
Valves	Poor fit between assembled valve parts	Major
	Scratched or marred fasteners or packing glands	Minor
	Gate valve: Gate off-center when viewed through open end	Major
	Fresh sand-blasted appearance of valve bodies, eyebolts, fittings and stems	Minor
	Loose or missing fasteners	Moderate
	Different design on valves of the same manufacturer	Moderate

Test/Materiel Type	Counterfeit Indicator	Strength of Indicator
	Some parts (e.g., hand wheels) look newer than the rest of the valve	Minor
	Excessive or missing markings (e.g. UL, FM, CGA, AGA)	Moderate
	Valves will not open or close, even when wrench applied	Major
	Substandard valves mixed in with standard valves (substitution)	Major
	Indications of prior use	Major
	Wrong/insufficient logo, , pressure rating, heat treat conditions, etc.	Major
	Altered markings on identification tags	Major
Small Hardware	Poor thread form, evidence of wear, or dressing	Moderate
	No markings for nuts or washers manufactured to a code or MIL-SPEC which requires marking	Major
	Headmarkings are marred, missing, or appear to have been altered	Major
	Headmarkings are inconsistent with heat/lot	Major
	Double stamping (Metric and SAE)	Major
	Headmarks with raised marks and depressed marks on same bolt	Major
Roller Bearings	Missing markings	Major
	Markings in wrong location	Moderate
	Evidence of re-stamping	Major
	Wrong material	Major
	Dimensional specifications out of tolerance	Major
	Incorrect packaging	Moderate

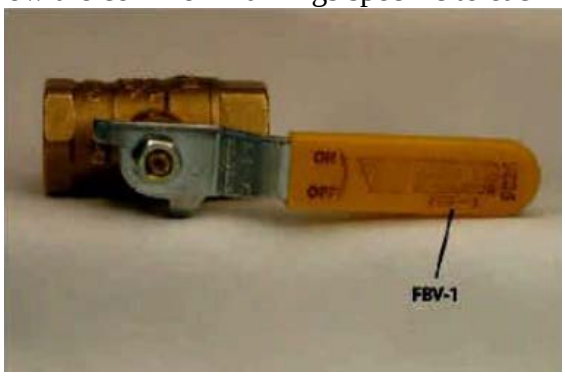
This page intentionally left blank

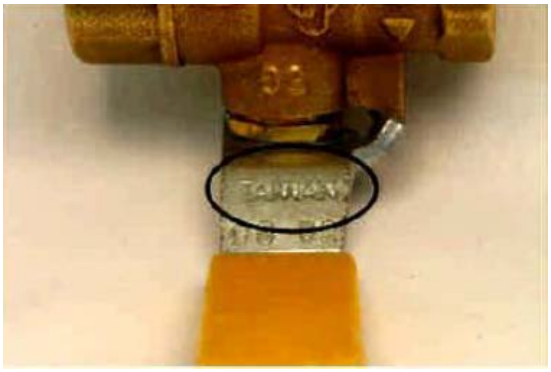
Appendix I: Examples of Counterfeit Mechanical Parts and Materials

- Counterfeit precision bearings had different packaging, dimensions, and lot/date code markings.



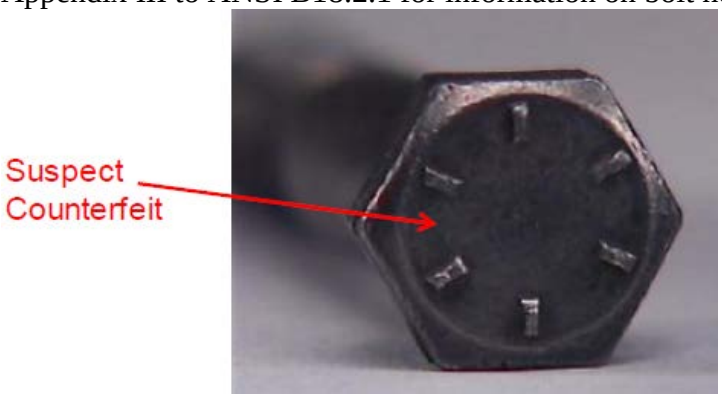
- Counterfeit valve, handle marked Watts Regulator FBV-1 but Watts doesn't manufacture a FBV-1 series valve. Further, Taiwan is stamped on the handle and Watts doesn't have a facility in Taiwan. It is important to know the common markings specific to each Valve manufacturer.



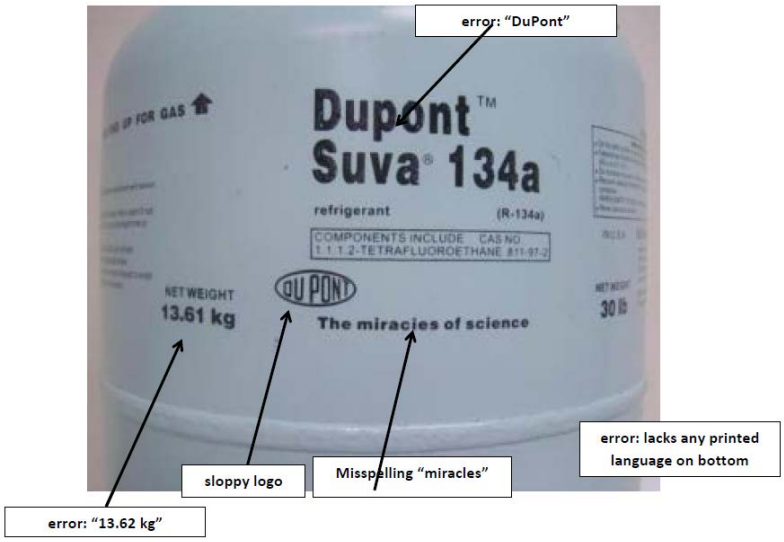


- Counterfeit valve was sold as “new” but was dirty, scratched, had clamp marks, had groove in bolt hole and had different rivet sizes on tag.

- Grade 8 bolts are the most commonly counterfeited fastener. No manufacturer’s mark or grade mark (unless certified to a specification not requiring marking) are visual indicators the part may be counterfeit. See Appendix III to ANSI B18.2.1 for information on bolt head markings based on the grade of the fastener.



- Counterfeit refrigerant gas had many print errors on the container. Counterfeit refrigerant (R-40 instead of R-134a) can cause cancer, kidney/liver damage, and corrosion to aluminum causing potentially a violent explosion.



- Counterfeit circuit breakers had different markings than genuine parts.

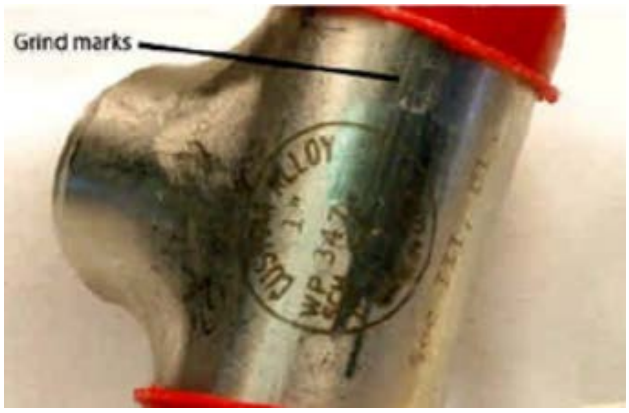
- Counterfeit pipe plugs were required to be 316 stainless steel and failed magnetic permeability testing. Full metallurgical analysis showed materiel is carbon steel. Further, manufacturer's marking did not match any in MIL-HDBK-57.

- Counterfeit bronze pipe tee's - material was found to be highly magnetic and rusted. Full metallurgical analysis found materiel is actually carbon steel painted a bronze color.

- Counterfeit hook – Crosby Group, Inc. has the patent trademark registration for the color Red in the United States. This hook was received from a Crosby distributor and represented as a Crosby hook. However, it was marked as “ELD” not “CG” or “Crosby”

- Counterfeit washers/spacers were received in the same box together. The counterfeit part had no marking and unknown manufacturer.

- Counterfeit stainless steel “T” weldlet had grind marks where information was removed and new information was stamped on.



This page intentionally left blank

Appendix J: Contractor Compliance Audit Checklist (Counterfeit Materiel)

Below are the sections and question listing for the Contractor Compliance Audit Checklist (Counterfeit Parts and Materials), based on MDA's contractor assessment process. There is also a listing of the significance of each question (2 – fairly insignificant, 3 – moderately significant, 4 – fairly significant, 5 – very significant, 5 – critical). These factors can be modified, and the score for each section, as well as overall score, will continue to be 100 as a maximum. Guidance is also provided in the checklist as to how to rate each question from 0 to 5. A low score for a highly significant question will impact the contractor's score more so than the same rating for an insignificant question. A sample of the rating guidance is provided in this appendix. This checklist is only useful if implemented in an excel file which can calculate a final score. This checklist is tailored significantly towards assessing the counterfeit electronic parts risk, but does include some assessment of non-electronic parts and materials. NOTE: An electronic copy of checklist can be obtained from the ASN(RD&A) website under policy documents.

Audit Checklist Sections, Questions, and Significance Factors

Q#	Section/Question	Significance
	Supplier Approval	
A1	Does the process for adding suppliers include appropriate supplier forms with specific reference to counterfeit avoidance and detection?	2
A2	Does the process for adding suppliers include verification of the supplier's selection and rating system to ensure the risk of low-quality or counterfeit parts is addressed?	3
A3	Does the process for adding suppliers include checking contractor history with the supplier, as well as checking government or commercial databases such as GIDEP and ERAI?	5
A4	Does the process for adding suppliers include checking of business information such as BINCS, DUNS, and SAM)?	5
A5	Does the process for adding suppliers include verification of ISO9001 and/or AS9120 certification?	2
A6	Does the process for adding suppliers include verification of membership in ERAI and/or IDEA?	3
A7	Does the process for adding suppliers include verification or requirements that the supplier's parts procurement strategy is to procure from an OM or authorized supplier instead of an unauthorized supplier?	5
A8	Does the process for adding suppliers include verification of compliance or certification to ANSI ESD S20.20 and IPC-J-STD-033?	4
A9	Does the process for adding suppliers include verification of minimum inspection and test requirements for all parts bought from unauthorized suppliers? What are the minimum requirements?	5
A10	Does the process for adding suppliers include verification of procedures to contain suspect and confirmed counterfeit parts?	3
A11	Does the process for adding suppliers include verification of procedures to	3

Q#	Section/Question	Significance
	report suspect and confirmed counterfeit parts?	
A12	Does the process for removing or restricting suppliers include periodic review of contractor quality data?	5
	Supplier Selection	
B1	Does the contractor maintain an approved supplier listing (ASL) with documented criteria for adding, removing, and rating suppliers?	5
B2	Does the contractor approved supplier listing separate authorized and unauthorized suppliers in a manner that facilitates selection of an authorized supplier first?	3
B3	Does the purchasing process require selection of parts from authorized suppliers as the first priority?	10
B4	Does the contractor's purchasing department verify a selected supplier is authorized by the OM to sell the parts?	5
B5	Does the purchasing process check GIDEP information for risky part numbers and suppliers?	5
B6	Does the purchasing process require customer notification and/or approval when unauthorized suppliers are to be used?	5
B7	Does the purchasing process require providing the customer with documented justification, traceability, and test plan (and results) when unauthorized suppliers are to be used?	5
B8	Does the purchasing process require documented traceability to an authorized supplier and the OM Certificate of Conformance?	5
B9	Are there contractual clauses which define supplier liability if counterfeit parts are encountered?	3
	Detection	
C1	Does the purchasing process require inspection to IDEA-STD-1010 (or equivalent) for all unauthorized supplier purchases for counterfeit part indicators? Is this performed by the supplier, contractor, or test lab?	10
C2	Does the purchasing process require marking and surface finish permanency testing for all unauthorized supplier purchases, including acetone and other aggressive solvents (e.g., Dynasolve 750 and/or 1M2P)? Is this performed by the supplier, contractor, or test lab?	10
C3	Does the purchasing process require minimum authenticity testing per MDA PMAP Table 5? Is this performed by the supplier, contractor, or test lab?	10
C4	Does the process identify parts bought from unauthorized suppliers to quality personnel at receiving and inspection?	4
C5	Do inspectors at the facility perform special inspections or tests when parts are bought from unauthorized suppliers?	3
C6	Does the contractor's process require further analysis of suspect counterfeit parts, including contacting the OM?	4
C7	Is there a percent defective allowable (PDA) specified when parts are bought from unauthorized suppliers that require further analysis before using parts which exceed the defect limit?	5
	Part Handling, Storage, Traceability, and Test	
D1	Are parts handled and stored in a manner compliant to ANSI ESD S20.20	5

Q#	Section/Question	Significance
	and IPC-J-STD-033 or equivalent?	
D2	Are parts for MDA managed and stored to allow full traceability to the part lot and/or date code?	4
D3	Do test failure analysis processes include consideration of whether parts were bought from unauthorized suppliers?	4
D4	Does the supplier maintain part traceability records for commercial items for mission critical items?	3
	Containment	
E1	Does the supplier have policies or procedures in place to prohibit the return of suspect and confirmed counterfeit parts to the supplier?	5
E2	Are suspect or confirmed counterfeit parts contained in a limited-access area, separate from good parts?	5
E3	Do processes call for containment of all affected product when parts are suspect or confirmed counterfeit?	5
E4	Do processes preclude the scrap or disposal of counterfeit parts without customer approval?	4
E5	Has the contractor found any counterfeit electronic parts in MDA mission critical systems?	N/A
	Reporting	
F1	Are there processes or procedures that require reporting to the customer if it is determined that parts installed in the customer's product are suspect or confirmed counterfeit?	5
F2	Are there processes or procedures that require reporting suspect and confirmed counterfeit parts to GIDEP?	4
	Obsolescence Management	
G1	Does the contractor maintain an obsolescence management plan that uses predictive tools to identify upcoming obsolescence of electronic parts?	5
G2	Does the obsolescence management plan include provisions for notification of the customer when obsolescence will impact the customer's program?	5
G3	Does the contractor take steps to avoid obsolescence by qualifying multiple suppliers for electronic parts whenever possible?	3
	Training	
H1	Do program management, engineering, and quality personnel at the contractor's facility receive formal training about counterfeit parts?	4
H2	Do buyers at the contractor's facility receive formal training about counterfeit parts and how to avoid them?	5
H3	Do inspectors at the contractor's facility receive formal training about counterfeit parts and how to detect them?	5
	Subcontractor Flow Down Verification	
I1	Does the contractor maintain a subcontractor compliance assessment schedule for all suppliers of mission and safety critical hardware?	10
I2	Does the contractor have documented criteria for defining suppliers of mission and safety critical hardware?	5
I3	How well does the contractor flow the supplier approval items in Section B to the critical subcontractors?	3

Q#	Section/Question	Significance
I4	How well does the contractor flow the detection items in Section C to the critical subcontractors?	3
I5	How well does the contractor flow the containment items in Section E to the critical subcontractors?	3
I6	How well does the contractor flow the reporting items in Section F to the critical subcontractors?	3
I7	How well does the contractor flow the training items in Section H to the critical subcontractors?	3
	Customer Flow Down Verification	
J1	Does the contractor's customer flow down explicit notification requirements for purchases from unauthorized suppliers?	N/A
	Mechanical Parts and Materials Anti-Counterfeit Processes	
K1	Does the contractor's purchasing process also include assessing mechanical part suppliers for counterfeit risk?	4
K2	Does the contractor's purchasing process also include assessing material suppliers for counterfeit risk?	4
K3	Are mechanical parts and materials traced back to the manufacturer through documentation?	3
K4	Are there particular inspections and tests defined for authentication of mechanical parts and materials?	3
K5	Do the contractor's containment requirements above also apply to mechanical parts and materials?	3
K6	Do the contractor's reporting requirements above also apply to mechanical parts and materials?	3

Audit Checklist Guidance (Partial Listing)

Q#	Section/Question	Rated 0	Rated 1	Rated 2	Rated 3	Rated 4	Rated 5
	Supplier Approval						
A1	Does the process for adding suppliers include appropriate supplier forms with specific reference to counterfeit avoidance and detection?	No forms for assessing suppliers.	Forms exist, but no reference to counterfeit parts.	Forms mention counterfeit parts in a general, non-specific way.		Forms specifically mention counterfeit parts, but don't address both avoidance and detection.	Forms specifically mention counterfeit parts, both for avoidance (supplier's selection of suppliers) and detection (inspections/tests performed by supplier).
A2	Does the process for adding suppliers include verification of the supplier's selection	No mention is made of a supplier ASL (Approved Supplier	Process confirms the supplier has a rating method for its	Process confirms there is a rating method to at least the level	Process confirms there is a rating method which includes	Process confirms there is a multi-level rating method	Process confirms there is a multi-level rating method

	and rating system to ensure the risk of low-quality or counterfeit parts is addressed?	Listing).	suppliers.	of "approved" and "disapproved".	approved, disapproved, and provisional.	which also checks GIDEP and ERAI reports.	which checks GIDEP and ERAI reports, along with peer complaint blogs.
A3	Does the process for adding suppliers include checking contractor history with the supplier, as well as checking government or commercial databases such as GIDEP and ERAI?	No checking of contractor history is performed.	Only local contractor history is checked.	Local contractor history is checked, along with GIDEP history.	Local contractor history, along with GIDEP and ERAI history.	Supplier history is checked throughout all contractor facilities, along with GIDEP and ERAI history.	Supplier history is checked throughout all contractor facilities, along with GIDEP and ERAI history. Documented rating guidance.
A4	Does the process for adding suppliers include checking of business information such as BINCS, DUNS, and SAM?	No checking of business history.	Not all of the business information is checked. There is no process.	Two of the pieces of information are checked per a documented process.	Two of the pieces of information are checked per a documented process at least annually.	BINCS, DUNS, and SAM information is checked per a documented process, at least semi-annually.	BINCS, DUNS, and SAM information is checked per a documented process, at least semi-annually. There are defined thresholds for acceptance.
A5	Does the process for adding suppliers include verification of ISO9001 and/or AS9120 certification?	No verification of either certification.	Documents if supplier is certified, but no requirements.		Requires ISO9001 or AS9120 certification.	Requires ISO9001 and AS9120 certification.	Requires at least one certification, and confirms validity through on-site audits.
A6	Does the process for adding suppliers include verification of membership in ERAI and/or IDEA?	No verification of membership.		Documents membership, but no requirements.			Requires supplier to be an ERAI or IDEA member.

This page intentionally left blank

Appendix K: Glossary of Terms

1 Approved Supplier. A supplier of parts that has been assessed by the approving organization (e.g., government, contractor) and determined to be an acceptable supplier for the organization. An approved supplier can be an Original Manufacturer (OM), authorized supplier, or unauthorized supplier, value-added supplier, etc.

2 Authenticate. The process of using inspections, tests, or other methods to determine whether a part or materiel has been knowingly misrepresented by a contractor or supplier and is considered a counterfeit part or materiel. Parts or materiels which have passed the authenticity process are considered to be authentic, valid versions of items.

3 Authorized Supplier. A supplier of parts that is within the terms of an OM contractual agreement. Contractual agreement terms include, but are not limited to, distribution region, distribution products or lines, chain of custody to the OM, licensed manufacturer, and/or warranty flow down from the OM. Authorized suppliers include the OM, a source with the express written authority of the OM or current design activity, and an authorized aftermarket manufacturer. Authorized suppliers are sometimes referred to franchised suppliers, franchised distributors, or authorized distributors.

4 Contractor. A supplier of assembled product. In the context of this document, a contractor is an organization that provides assembled product under a Department of Navy (DON) contract. This includes subcontractors that supply product to contractors that are under DON contract.

5 Contractor Approved Supplier. A supplier that does not have a contractual agreement with the original component manufacturer for a transaction, but has been identified as trustworthy by a contractor or subcontractor.

6 Counterfeit Materiel. Items that are unauthorized copies or substitutes that have been identified, marked, or altered by a source other than the items' legally authorized supplier or have been misrepresented to be authorized items of the legally authorized supplier. Examples include but are not limited to:

- Used materiel sold as new.
- Materiel represented as having specific capability (e.g., speed, power, temperature, capacity) beyond what the part was tested to by the OM.
- Material construction (e.g., anodization, composition) other than the materiel's advertised construction.

7 Critical Materiel. Critical Materiel includes Critical Safety Items (CSI), Critical Application Items (CAI), Controlled Inventory Items (CII), Information and Communications Technology (ICT) Components and:

- Other materiel identified by the responsible engineering support activity prior to initial supportability analysis and documented by the responsible logistics organization. Initial

supportability analysis occurs either during the initial provisioning and cataloging process or upon approval of a design change notice.

- Materiel that is at high risk of counterfeiting as determined by either the responsible engineering support activity or by the program management office. Electronic semi-conductors and microchips are generally considered high risk depending on type and application.

8 Electronic Part. An integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly.

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

10 High Risk. Materiel that has previously been counterfeited or is susceptible to counterfeiting and has an end use or application where the success or security of the mission, or safety of the warfighter, depends on the continued reliable function of the materiel. At this time, materiel at high risk of counterfeiting includes:

- Integrated circuits
- Discrete semiconductors (e.g., transistors, diodes, optocouplers)
- High voltage, high value, or specialty (e.g., low ESR, high Q, trimmer) capacitors
- Mechanical roller bearings
- Specialty fasteners
- Lubricants
- Adhesives
- Batteries
- Other materiel identified in Government-Industry Data Exchange Program (GIDEP) or Product Data Reporting and Evaluation Program (PDREP) reports as susceptible to being counterfeited.

11 Industry Standards. A set of criteria within an industry relating to the standard functioning and carrying out of operations in its respective field of production. Generally accepted requirements followed by the members of an industry. It provides an orderly and systematic formulation, adoption, or application of standards used in a particular industry or sector of the economy. Industry standards vary from one industry to another. A list of key industry standards is provided in enclosure (3).

12 Integrated Circuit. A collection of discrete electronic components combined into a single package to perform a system function, such as to amplify, process, or store data.

13 Information and Communications Technology. Includes all categories of ubiquitous technology used for the gathering, storing, transmitting, retrieving, or processing of information (e.g., microelectronics, printed circuit boards, computing systems, software, signal processors, mobile telephony, satellite communications, and networks). ICT is not

limited to information technology (IT), as defined in section 11101 of title 40, U.S.C. Rather, this term reflects the convergence of IT and communications.

14 Materiel. Material, system components, sub-components, software, and information and communications technology. Materiel includes support equipment and systems purchased, procured, contracted, or incorporated into the DOD supply chain for weapon and information systems, DOD business processes, and DOD operational support.

15 Original Manufacturer. An organization that designs and/or engineers a part or materiel and is pursuing or has obtained the intellectual property rights to that part. This may include authorized aftermarket manufacturers who have contracted with the OM of the part to continue production.

16 Product Data Reporting and Evaluation Program (PDREP). The DON program that supports requirements regarding the reporting, collection and use of supplier performance information identified in the Code of Federal Regulations (CFR), Federal Acquisition Regulations (FAR), Defense Federal Acquisition Regulation Supplement (DFARS) and DON regulations. PDREP supports DON management of the supply chain ensuring first time quality and on-time delivery of materiel for both critical and non-critical applications.

17 Product Quality Deficiency Report (PQDR). A report format within the DON PDREP program for documenting defective or nonconforming materiel. The defect code '5AS' is reserved for documenting suspect or confirmed counterfeit materiel.

18 Risk-Based Approach. An analytical strategy that focuses attention on areas or applications where failures will produce severe consequences and trigger impacts to the overall mission objectives and/or human safety.

19 Supplier. A supplier of materiel. In the context of this document, a supplier is not a contractor or the manufacturer or intellectual property rights holder of the materiel, but is an organization that supplies materiel to the contractor or DON organization. References to supplier audits apply primarily to unauthorized sources, for which the greatest risk of counterfeit materiel exists.

20 Suspect Counterfeit Materiel. Materiel, item, or product in which there is an indication by visual inspection, testing, or other information that it may meet the definition of counterfeit materiel provided instruction.

21 Unauthorized Supplier. A supplier of parts that is not within the terms of an OM contractual agreement. Unauthorized suppliers usually sell materiel that has not been obtained from the OM or an authorized supplier. This is the riskiest supplier in terms of counterfeit risk. Unauthorized suppliers are frequently referred to as independent distributors or brokers.

This page intentionally left blank

Appendix L: List of Acronyms

AGA – American Gas Association
ANSI – American National Standards Institute
ASL - Approved Supply Listing
ASN(RD&A) - Assistant Secretary of the Navy Research, Development and Acquisition
BINCS - Business Identification Number Cross-Reference System
CAI - Critical Application Item
CAR - Corrective Action Request
CAS - Cost Accounting Standards
CDRL – Contract Data Requirements List
CFR - Code of Federal Regulations
CGA – Canadian Gas Association
CII - Controlled Inventory Item
CMM - Coordinate Measuring Machine
CoC - Certificate of Conformance
CPI - Critical Program Information
CSAM – C-Mode Scanning Acoustic Microscopy
CSI - Critical Safety Item
DAS – Defense Acquisition System
DC – Date Code
DFARS - Defense Federal Acquisition Regulation Supplement
DID - Data Item Description
DLA - Defense Logistics Agency
DLAR – Defense Logistics Agency Regulation
DMSMS - Diminishing Manufacturing Sources and Material Shortages
DNA - Deoxyribonucleic Acid
DOD – Department of Defense
DON - Department of Navy
DPA – Destructive Physical Analysis
DUNS - Data Universal Numbering System
ECIA – Electronic Components Industry Association
ECP – Engineering Change Proposal
EDS – Energy Dispersive Spectroscopy
EEE – Electrical, Electronic, and Electromechanical
ESD – Electrostatic Discharge
FAR - Federal Acquisition Regulations
EU – European Union
FSC - Federal Stock Classification
FSG - Federal Supply Group
FTIR - Fourier Transform Infrared Spectroscopy
GIDEP - Government-Industry Data Exchange Program
GPC - Government Purchase Card
HIC – Humidity Indicator Card
ICP-AES - Inductively Coupled Plasma-Atomic Emission Spectroscopy
ICT - Information and Communications Technology
IDEA – Independent Distributors of Electronics Association
IPC - Association Connecting Electronics Industries

ISO – International Standards Organization
IT – Information Technology
J&A - Justification and Approval
JCIDS - Joint Capabilities Integration and Development System
JFAC - Joint Federated Assurance Center
LCSP – Life Cycle Sustainment Plan
MDA – Missile Defense Agency
MRB – Material Review Board
MS – Mineral Spirits
NCIS - Naval Criminal Investigative Service
NRTL – Nationally Recognized Test Laboratory
NSWC – Naval Surface Warfare Center
NWRM- Nuclear Weapons Related Materiel
OM - Original Manufacturer
OMB – Office of Management and Budget
OSD - Office of the Secretary of Defense
PDA - Percent Defective Allowable
PDR - Preliminary Design Review
PDREP - Product Data Reporting and Evaluation Program
PMAP – Parts, Materials, and Processes
PPP – Program Protection Plan
PQDR - Product Quality Deficiency Report
RFQ – Request For Quotation
RMP – Risk Management Plan
RTA - Requiring Technical Authority
SAE – Society of Automotive Engineers
SAM - System for Award Management
SAP - Simplified Acquisition Procedures
SASL – Supplier's Approved Supplier Listing
SEM - Scanning Electron Microscopy
SEP – Systems Engineering Plan
SETR – Systems Engineering Technical Review
SOW - Statement of Work
SUA – Supplier Under Assessment
TPOC – Technical Point of Contact
TSN - Trusted Systems and Networks
UL – Underwriters Laboratory
UPC – Universal Product Code
WDS – Wavelength Dispersive Spectroscopy
XPS - X-ray Photoelectron Spectroscopy
XRF - X-ray Fluorescence

Appendix M: Reference Documents

The following documents are either referenced in this document or were used in its development.

a. SECNAVINST 4855.20, Counterfeit Materiel Prevention of 22 April 2015
b. DODI 4140.67, DoD Counterfeit Prevention Policy of 26 April 2013
c. SD-22, Diminishing Manufacturing Sources and Material Shortages A Guidebook of Best Practices for Implementing a Robust DMSMS Management Program of August 2012
d. SECNAVINST 4855.3, Product Data Reporting and Evaluation Program (PDREP) of 27 June 2014
e. Government Industry Data Exchange Program (GIDEP) Operations Manual, current revision
f. DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks of 5 November 2012
g. DODI 5000.02, Operation of the Defense Acquisition System of 7 January 2015
h. Program Protection Plan (PPP) of 18 July 2011
i. Defense Federal Acquisition Regulation Supplement, current edition
j. Assistant Secretary of the Navy Research, Development and Acquisition (ASN(RD&A)) DMSMS Management Plan Streamlining Guide, dated July 2016
k. DI-QCIC-80127A, GIDEP Annual Progress Report of 5 May 2003
l. DI-QCIC-80125B, GIDEP Alert/Safe-Alert Report of 5 May 2003
m. DI-QCIC-80126B, GIDEP Alert Response of 5 May 2003
n. DI-MISC-81832, Counterfeit Prevention Plan of 21 January 2011
o. NAVSO P-3683, Navy and Marine Corps Product Data Reporting and Evaluation Program of 5 April 2013
p. DLA Regulation (DLAR) 4155.24, Product Quality Deficiency Report Program of 20 July 1993
q. SECNAVINST 5000.2E, DON Implementation and Operation of the DAS and JCIDS 1 September 2011
r. SECNAVINST 4140.2, Management of Aviation Critical Safety items of 25 January 2006
s. DODM 4140.01 – DOD Supply Chain Materiel Management Procedures, Volume 11 of 8 March 2017