Headquarters
Department of the Army
Washington, DC
9 January 2023

Department of the Army
Pamphlet 702–20

Product Assurance

Counterfeit Risk Management Product Assurance Handbook

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

MARK F. AVERILL
Administrative Assistant to the Secretary of the Army

History. This publication is a new Department of the Army pamphlet.

Applicability. This pamphlet applies to the Regular Army, Army National Guard/Army National Guard of the United States and the U.S. Army Reserve, unless otherwise stated.

Proponent and exception authority. The proponent of this pamphlet is the Assistant Secretary of the Army (Acquisition, Logistics and Technology). The proponent has the authority to approve exceptions or waivers to this publication that are consistent with controlling law and regulations. The proponent may delegate this approval authority, in writing, to a division chief within the proponent agency or its direct reporting unit or field operating agency in the grade of colonel or the civilian equivalent. Activities may request a waiver to this publication by providing justification that includes a full analysis of the expected benefits and must include formal review by the activity's senior legal officer. All waiver requests will be endorsed by the commander or senior leader of the requesting activity and forwarded through their higher headquarters to the policy proponent. Refer to AR 25–30 for specific requirements.

Suggested improvements. Users are invited to submit comments and suggested improvements on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Deputy Assistant Secretary of the Army (Acquisition Policy and Logistics), usarmy.pentagon.hqda-asa-alt.list.saal-lp@mail.mil.

Distribution. This publication is available in electronic media only and is intended for the Regular Army, Army National Guard/Army National Guard of the United States, and the U.S. Army Reserve.

Contents (Listed by chapter and page number)

Chapter 1
Introduction

1–1. Purpose
Preventing counterfeit parts and material from entering the supply chain is achieved through proper execution of the procedures and requirements in this pamphlet. This pamphlet establishes guidance, functions, and procedures for implementing the U.S. Army's counterfeit risk management (CRM) product assurance. The goal of this pamphlet is to reduce, prioritize, identify, and avoid the risk of counterfeit parts and material entering into the field. This pamphlet is organized to provide detailed guidance for implementation of AR 702–20.

1–2. References, forms, and explanation of abbreviations
See appendix A. The abbreviations, brevity codes, and acronyms (ABCAs) used in this electronic publication are defined when you hover over them. All ABCAs are listed in the ABCA database located at https://armypubs.army.mil/abca/.

1–3. Associated publications
Policy associated with this pamphlet is found in AR 702–20.

1–4. Records management (recordkeeping) requirements
The records management requirement for all record numbers, associated forms, and reports required by this publication are addressed in the Records Retention Schedule–Army (RRS–A). Detailed information for all related record numbers, forms, and reports are located in Army Records Information Management System (ARIMS)/RRS–A at https://www.arims.army.mil. If any record numbers, forms, and reports are not current, addressed, and/or published correctly in ARIMS/RRS–A, see DA Pam 25–403 for guidance.

Chapter 2
Prevention

Section I

General

2–1. Overview
Army policy requires implementation of a risk-based approach to prevent the introduction of counterfeit parts and material into the supply chain. Preventative measures such as early detection processes, strengthened surveillance procedures, and accountable oversight are fundamental anti-counterfeit activities. Additionally, measures must be implemented for the removal and reporting of suspected and confirmed counterfeit parts and material from the system and supply chain.

2–2. Program framework
a. Objective. The Army's CRM product assurance framework is a structured approach designed to increase awareness and establish requirements in order to combat the counterfeit risk prevalent in the modern global supply chain. The practices, processes, procedures, and activities in this pamphlet are used to implement the program. Readiness risk issues can threaten the safety of the user and success of the mission.

(1) Counterfeit parts and materials are often inferior in quality and function, potentially leading to premature product failure.

(2) Used parts and material misrepresented as new, or an incorrect version misrepresented as the correct parts and material, may lead to a product with a lower mean time before failure than expected from a new part.

(3) Some counterfeit appears to be genuine, but has been modified or sabotaged either to cause premature failure or to gather information from the equipment when it is in use.

b. Desired outcomes and activities. The Army's CRM product assurance activities and desired outcomes are as follows:

(1) Create awareness and establish requirements to prevent procurement of counterfeit parts and material.

(2) Employ a risk-based approach to reduce the frequency and impact of counterfeit parts and material within DoD acquisition systems and DoD life-cycle sustainment.

(3) Apply prevention and early detection procedures to minimize the presence of counterfeit parts and material within the DoD supply chain.

(4) Mandate and require strong oversight and surveillance procedures for critical parts and material be included in each procurement action to prevent counterfeiting. For electronic parts, include DFARS clauses listed in AR 702–20.

(5) Document all occurrences of suspect and confirmed counterfeit in the appropriate reporting systems (see chap 4).

(6) Make information about counterfeiting accessible at all levels of the Army supply chain as a method to prevent further counterfeiting.

(7) Investigate, analyze, and assess all cases of suspected counterfeit parts and material.

(8) Notify the U.S. Army criminal investigative organizations and intelligence authorities and those who use the suspect and confirmed counterfeit parts and material of incidents at the earliest opportunity. Seek restitution for confirmed cases and obtain remedies prescribed by relevant authorities, including DoDI 7050.05 and the FAR Part 46.

(9) Conduct proper disposition of parts and material to ensure product is not reintroduced into the supply chain.

2–3. Life-cycle planning

Counterfeit risk affects a program's life cycle from the conception of design to end of useful life. It is imperative that an organization's personnel awareness encompasses the entire spectrum of a product's life cycle.

a. Figure 2–1 provides a life-cycle overview of typical risk management measures required to protect a program's readiness posture.

b. Supply chain risk management must be conducted over the entire life of a product, from the initial materiel solution analysis through the final disposition of the product.

(1) Initial acquisition management attempts to mitigate the threat of counterfeit by proactively creating processes to minimize future supply chain risks.

(2) Inventory management attempts to implement additional supply chain risk management processes through proper purchasing, inventory control, and disposal of purchased parts and materials.

c. The Life-Cycle Sustainment Plan (LCSP) for any new system must have information on how to mitigate the counterfeit risks in the parts and materials found in that system. The plan must include language on how the program will—

(1) Procure parts and materials from authorized suppliers.

(2) Inspect and test incoming parts and materials.

(3) Report suspected counterfeit to the appropriate parties and databases.

(4) Quarantine and disposition parts and material believed to be counterfeit.

d. An example of language that should be used in the LCSP is located in appendix E.

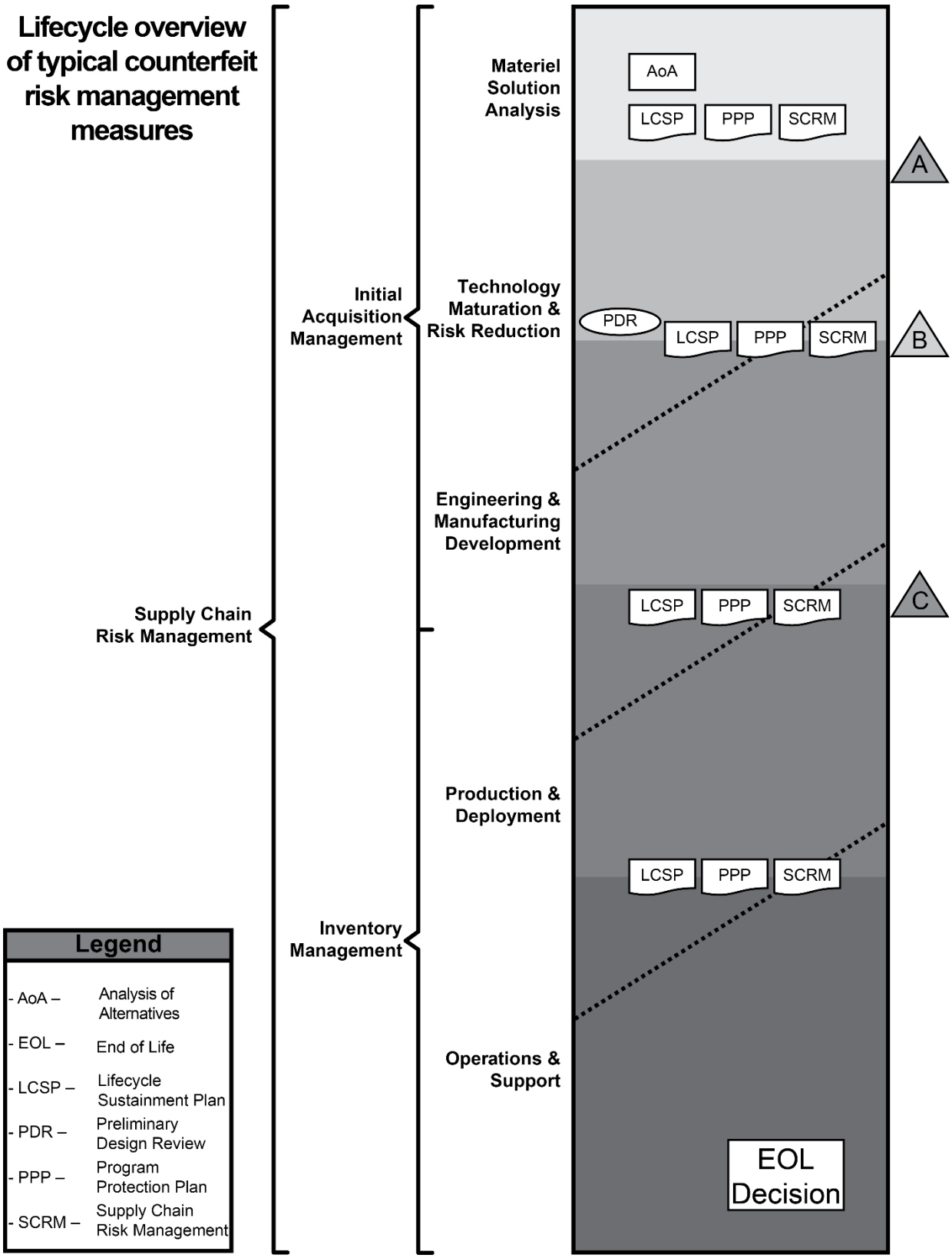

Figure 2–1. Life-cycle overview of typical counterfeit risk management measures

2–4. Milestone activities
See AR 702–20 for policy regarding milestone activities.

Section II

Training

2–5. Training overview
Training the workforce is critical to sustaining counterfeit prevention, detection, and mitigation of parts and materials within the DoD supply chain. This training must be available to any government personnel involved in the ordering, receiving, inspection, and issuance of parts and materials.

2–6. Training resources
Training resources are to be used to provide the necessary guidance across the Army supply chain. Various outlets for resources provide the necessary assistance to train proper workforce personnel in counterfeit prevention, mitigation, and detection practices.

a. Government-built training resources are designed to provide an overview of the counterfeit threat, as well as the Federal guidance and direction when creating location-specific and item-specific CRM processes. This level will have overarching guidance on purchasing and reporting parts and materials.

b. Defense Acquisition University available Logistics (LOG) counterfeit courses include:

(1) LOG 0320, Preventing Counterfeit Electronic Parts from Entering the DoD Supply Chain.

(2) LOG 0620, Counterfeit Prevention Awareness.

c. Organization-specific resources are to be created to provide standard processes and procedures for items procured, managed, or supported by that organization. The organization is responsible for their own guidance on specific inspection, testing, and parts and material control.

d. Non-governmental trainings, including contractor-led training sessions, may be used to provide specialized information applicable to item-unique or process-unique guidance. This guidance is to be used to supplement the Government-built and organizational-specific training resources.

2–7. Personnel requirements
The CRM requires personnel onsite to proactively prevent counterfeit threats from affecting the supply availability of parts and materials within the Army.

a. Counterfeit awareness training is needed for Army personnel providing support in the following areas:

(1) Contracting.

(2) Procurement.

(3) Receiving and/or inspection.

(4) Engineering support.

(5) Quality assurance.

b. The CRM basic awareness training will be available as needed for personnel who may come in contact with counterfeit parts and materials. Additional training beyond basic awareness training will be required for any location’s CRM point of contact (POC).

c. Each Life Cycle Management Command and major subordinate command will have a CRM POC to provide onsite support if counterfeit parts and materials are discovered. This POC will provide access to Government-Industry Data Exchange Program (GIDEP)/ Product Data Reporting and Evaluation Program (PDREP) and is responsible for creating the GIDEP/PDREP alerts when any counterfeit is found at his or her Army location.

Chapter 3
Risk Management

Section I

General

3–1. Overview
Risk of field failures due to counterfeit parts must be assessed for each Army system. Proper CRM requires appropriate prevention, detection, and mitigation to keep the warfighter safe. The CRM begins at the materiel solution analysis phase and ends at final system disposal. Throughout the life cycle, the system and components will be reviewed for counterfeit risks based on the following criteria:

a. Susceptibility of specific parts and materials to counterfeiting.
b. Difficulty in procuring key parts for the system.
c. Availability or lead time challenges for key system components.
d. Criticality of the part or assembly to the functionality of the system.
e. Fragility and criticality of key component suppliers.
f. Modularity of components within the system.

3–2. Impact
Counterfeit parts and materials can lead to decreased reliability, inability to function, and potentially to mission failure risks. Items that are susceptible to malicious counterfeiting or are critical to mission success must have prevention, detection, and mitigation measures in place.

a. Criticality. Items with higher criticality to completing missions provide a significant danger if they are counterfeit. Counterfeit parts are often sold as authentic, new items, but are actually refurbished, remarked parts. The lack of quality control combined with the inability to capture parts and material traceability can lead to inferior products, increasing the risk of mission failure and danger to the user. The program's engineering support activity (ESA) must identify and document what items are critical, in accordance with DoDI 5000.02 and DoDI 5200.44.

b. Strategic value. Parts and materials that could present an adversary with a specific strategic advantage are a target to be counterfeit. Malicious insertions are not limited to hardware, and include software and firmware. Malicious insertions can result in system data being reported to an adversary, monitoring of a system by an adversary, or enabling an adversary to control the system.

3–3. Likelihood
All parts and materials have the potential to be counterfeited. The likelihood of parts and materials being counterfeited increases when the item is experiencing diminishing manufacturing sources and material shortages (DMSMS). The following are the major risk factor triggers for materials and parts, with their description. When these occur, the materiel developer and U.S. Army Materiel Command personnel will conduct a review of existing anti-counterfeit measures to ensure they adequately address risk.

a. Obsolescence. After the original equipment manufacturer (OEM)/original component manufacturer (OCM) has discontinued production of the item and its spare parts, if demand is still high there is a risk of counterfeit. The parts and materials may only be available from unauthorized gray and black-market distributors. Both the parts and materials and the OEM/OCM documentation authenticating the parts and materials and providing supply chain traceability could be counterfeited.

b. Difficult to procure. Some materials or parts may present procurement challenges such as special waivers, rare materials, environmental concerns, and so forth. Falsification of documentation may allow noncompliant items to be sold fraudulently.

c. Lead time. Parts and material that has a long procurement lead time is susceptible to counterfeit in scenarios where schedule is critical. Counterfeit parts and materials often have shorter procurement lead times.

d. Item type. Historically, specific items have been identified as more likely to be counterfeit. A 2012 Defense Logistics Agency (DLA) assessment of counterfeit risk within DLA's supply chain examined 69 DLA-managed Federal Supply Groups (FSGs). See appendix C for entire list of FSGs broken out by risk levels. Of these 69 FSGs, the 5 most frequently counterfeit were:

(1) FSG 59. Electrical and electronic equipment components such as integrated circuits (ICs), transistors, diodes, connectors, and electronic assemblies.
(2) FSG 29. Engine accessories such as filters, valves, and pumps.
(3) FSG 47. Pipe, tubing, hose, and fittings.
(4) FSG 53. Hardware and abrasives such as nuts, bolts, washers, screws, brackets, seals, O-rings, lubricants, and abrasives.
(5) FSG 25. Vehicular equipment components such as brakes and springs.

e. Volume. Parts and materials that are required to be purchased in bulk or large quantities are susceptible to counterfeit as it presents an opportunity to reap a large profit, even if the profit margin on a single item is not significant.

f. Price. Parts and materials that have a high purchase price are considered high risk of counterfeit, as even a small volume purchase can provide significant profit, especially when the profit margin is large.

g. Commercial versions. Parts and materials with multiple versions, to include commercial and military versions that are visually the same but built to separate standards and specifications, are at risk of misrepresentation and counterfeit. Selling a lower quality part as the military variant increases profit margins for the supplier, and puts the end item's operation at risk. Additionally, commercial versions are more likely to exist in the recycle stream and have a risk of re-entering the supply chain refurbished and misrepresented as military versions. An example might be a common bolt or washer that is available in several different plating or heat treatment versions, or an IC with commercial, industrial, and military temperature ranges available. In these cases, lower-quality or lesser parts can be sold for a higher price.

h. Certification. Parts and materials that require specific documentation and certification are at risk of counterfeit, as fraudulent and falsified documents could be presented to support acceptance of parts and materials that do not conform to specifications.

i. Strategic value. Parts and materials that could present an adversary with a specific strategic advantage are a target to be counterfeit.

j. Additive manufacturing. Any item that may be created by an unauthorized source using additive manufacturing. If the item can be created using additive manufacturing, it can be exploited by non-authorized sources looking to make a profit or to maliciously modify features within the item.

Section II

Supplier Selection

3–4. General

The most reliable source of supply for all parts and material is the OEM, OCM, or authorized aftermarket manufacturer (AAM). If the required parts and materials are not procurable from one of these three sources, then the source of supply needs to be thoroughly vetted and determined to be a low risk supplier prior to parts and material acquisition. Conducting a risk assessment of an unauthorized supplier requires the consultation and concurrence of the technical authority. Paragraph 3–8 details processes for reviewing unauthorized suppliers.

3–5. Supplier types

a. DFARS 246.870–2 requires all contractors and subcontractors to obtain in-production electronic parts from the OEM, OCM, or an AAM. If the electronic parts are no longer in production, and are not available from the OEM, OCM, or an AAM, they may be procured from suppliers identified as contractor-approved suppliers, subject to the contractor's use of established counterfeit prevention industry standards and processes, contractor assumption of responsibility of part authenticity, and Government review, audit, and approval.

b. DFARS 246.870–2 requires electronic parts or products contractors and their subcontractors who are subject to the cost accounting standards to employ a counterfeit electronic part detection and avoidance system. The counterfeit electronic part detection and avoidance system requirements are outlined in DFARS 246.870–2(b)(2). It is recommended that these requirements be applied to all procuring organizations and all types of parts and materials.

c. Independent of any other factor impacting the likelihood an item being counterfeit, the strongest indicator of parts and material authenticity prior to acquisition is the trustworthiness of the supplier. DFARS

252.246–7008 defines the following sources of electronic parts, divided into three levels based on trustworthiness.

(1) *Level 1. Authorized manufacturers.*

(a) Original equipment manufacturer. A company that manufactures products that it has designed from purchased components and sells those products under the company's brand name. The OEMs usually offer warranty for their parts and parts and materials, to include replacement cost, technical assistance, counterfeit testing and other support. An OEM is the lowest risk supplier.

(b) Original component manufacturer. An organization that designs and/or engineers a part and is entitled to any intellectual property rights to that part. The OCMs usually offer warranty for their component, to include replacement cost, root cause analysis, counterfeit testing and other technical assistance. An OCM, like the OEM, is the lowest risk supplier.

(c) Authorized aftermarket manufacturer. An organization that fabricates a part under a contract with, or with the express written authority of, the OCM based on the OCM's designs, formulas, and/or specifications. The AAM production usually occurs after the OEM/OCM discontinues production despite a continued requirement for the item. The risk of procuring counterfeit parts and materials from an AAM is low, similar to an OEM/OCM, and the item will usually include a warranty.

(2) *Level 1A. Authorized suppliers and/or distributor.* A supplier, distributor, or an aftermarket manufacturer with a contractual arrangement with, or the express written authority of, the original manufacturer or current design activity to buy, stock, repackage, sell, or distribute the part. In an authorized supply chain, the supplier and/or distributor should honor the OEM/OCM/AAM's warranty. A supplier's authorization should be confirmed by the OEM/OCM/AAM for each product to be procured from the supplier. Authorized suppliers have a low risk of providing counterfeit parts and material, but the risk is greater than direct procurement from the OEM/OCM/AAM. The increased risk can be mitigated by careful confirmation with the OEM/OCM/AAM that the source of supply is truly an authorized supplier for that specific item, and confirming with the authorized supplier that the item has not been previously shipped then returned from a previous customer.

(3) *Level 2. Unauthorized suppliers: brokers, independent distributors, gray market suppliers.* These suppliers do not have a contractual agreement with the OEM/OCM/AAM for a transaction. These suppliers often cannot confirm that a part is new or previously unused and that it has not been commingled, mixed, or blended in supplier new production or stock with used, refurbished, reclaimed, or returned parts. Unauthorized suppliers are extremely high risk. They are never to be used as a source of supply if the parts and materials are available directly from the OEM/OCM/AAM or an authorized supplier. A subcontractor that refuses to accept the flow-down of DFARS 252.246–7008 is also considered an unauthorized supplier and high risk.

d. Figure 3–1 summarizes the three levels of supplier types. Authorized suppliers and unauthorized suppliers can overlap, as an authorized supplier for one product, while being an unauthorized supplier for other products. In this scenario, these authorized suppliers are considered high risk. Parts and materials procured at high risk are to be supported by an approved supplier list (ASL), provided that the ASL is carefully produced and updated at a regular interval. All suppliers included on the ASL will be identified by their supplier type. Inclusion of an unauthorized supplier on an ASL does not preclude the procuring organization from notifying the contracting officer if that supplier is chosen as the source of supply.

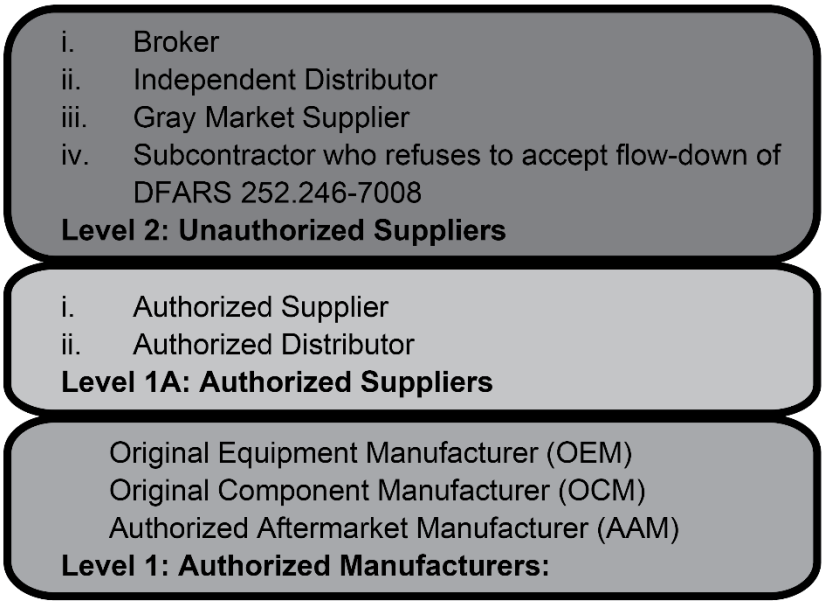

Figure 3–1. Supplier levels

3–6. Risk assessment

The impact risk is the risk to product functionality, Soldier safety, and mission success. Due to impact risks of counterfeit on items procured, a risk assessment, as required by AR 702–20, will be conducted prior to purchasing parts and materials.

a. Various parts and materials have different functions on Army equipment and can cause more significant issues with product failure.

b. Items with high strategic value or criticality for mission functionality will have a higher impact and must have reviews that are more rigorous prior to sending into the field.

c. Risk and impact for specific items are to be defined by the program manager for each product as necessary.

d. See appendix B for guidance when conducting assessments discussed in this document and AR 702–20.

3–7. Order of procurement from supplier by type

When suppliers provide parts and materials, there is an inherent risk of counterfeit being introduced into the Army supply chain. To minimize the risks in the procurement process, use the following steps:

a. The first source of parts and material procurement is always OEMs, OCMs, or AAMs, since these manufacturers have part and material traceability from initial item creation.

b. If parts are not procurable from OEMs, OCMs, or AAMs, an authorized supplier of the desired part or material will be contacted for current authentic, traceable stock of the needed items. Alternatively, redesign may be conducted to determine if parts and materials may be replaced or removed from the overall equipment design.

c. If the needed items are not available from authorized suppliers, additional suppliers from an organizational approved suppliers list are to be contacted. These ASLs may be government or contractor owned, but must be available to the Government at any time, upon request.

d. If no approved suppliers have the items available, unauthorized suppliers may be used, with appropriate testing and inspection procedures followed for procured parts and materials. The item's ESA or Defense Contract Management Agency (DCMA) must be aware of the supplier issue and review the proposed supplier's counterfeit prevention process. Upon satisfactory review by the ESA, proper inspection and testing procedures may be implemented for the order. Proper inspection and testing must be done prior to fielding equipment with parts and materials procured from this order.

e. Items acquired from unauthorized, unapproved suppliers are considered a last resort option, and must follow the same procedure as unauthorized approved suppliers. Additionally, the item's program manager is to be notified of the lack of approved manufacturers for current and future purchases of the needed parts and materials.

3–8. Reviewing unauthorized suppliers

The steps discussed in this paragraph to review unauthorized suppliers are not all-encompassing and should not be used as sole justification for approval of a purchase from an unauthorized supplier. This paragraph is designed to provide basic guidance when reviewing unauthorized suppliers prior to purchasing any parts or materials. This paragraph does not supersede any FAR, DFARS, or Office of the Secretary of Defense directive on purchasing parts and materials from unauthorized suppliers. See DoDI 4140.01 and DFARS 252.246–7008 for additional guidance on parts management.

a. If the supplier provided any parts or materials to the Government in the past, their acceptance rate is to be reviewed by the contracting officer. A larger number of sales without incident provides the Government a greater confidence in the supplier.

b. The supplier will be verified through GIDEP and PDREP, as well as any other accessible database containing counterfeit notices, to confirm they have no recorded history of providing counterfeit parts and materials to any customers. Additionally, GIDEP and PDREP will be used to confirm supplier has no outstanding quality issues on any orders with the Government.

c. The supplier will have an approved suppliers list of their own suppliers available for Government review.

(1) The supplier will provide, upon request, companies on approved suppliers list with a history of issues meeting delivery needs.

(2) The supplier list will include a listing of companies excluded due to counterfeit or other quality issues.

(3) The supplier will provide, upon request, their quality assurance certificate documents to increase the justification of confidence of the parts.

d. The supplier will be able to provide traceability of the parts and materials being sold to the Government. If the supplier is unable to provide traceability, the supplier will document their source of supply, with contact information, and provide justification of confidence that parts or materials are authentic.

3–9. Procurement

For all procurements, the ESA must identify electronic parts and any critical parts that need counterfeiting protections. The ESA must provide the required verification procedures to be used to verify compliance to the technical requirements. The procurement officer must incorporate those requirements into the procurement contracts to include the DFARS counterfeiting clauses. The proper contract data requirements lists (CDRLs) and data item descriptions (DIDs) for electronic parts must also be added during the contract phase to receive data to aid in verification of compliance.

a. The procurement officer and ESA will conduct market research to determine an acceptable source of supply.

b. The prime contractor will be required to flow-down DMSMS management requirements to include the engineering bill of materials/parts lists, as well as item traceability and quality requirements, to their subcontractors.

c. The prime contractor will comply with the contractual CDRLs and DIDs as required to mitigate counterfeit risk while ensuring compliance with all applicable DFARS provisions, DoD issuances, Army regulations, and DMSMS requirements pertaining to the risk of acquiring counterfeit parts. A Counterfeit Prevention Plan that addresses the requirements of SAE AS5553 and SAE AS6174 will be required with Government approval.

d. For higher risk components, items with a critical function, and items critical to the safety of the user that are available only from unapproved/unproven sources, a testing plan will be developed that mitigates

the likelihood of acquiring counterfeit items. Specific inspection and testing practices are provided in standards SAE AS5553, SAE AS6081, SAE AS6171/1, SAE AS6171, and SAE AS6174, and IDEA–STD–1010.

e. In scenarios where a part is not available from the OEM/OCM, AAMs, or authorized distributors, purchases must be made from a supplier on an ASL. Prior to placing a purchase order with a nonauthorized supplier, the purchaser will check both the GIDEP and PDREP databases to confirm that the proposed supplier has not previously supplied counterfeit parts.

f. Review and evaluate alternative procurement options such as the following before purchasing from an unauthorized supplier:

(1) Long-term buy.
(2) Lifetime buy possibilities.
(3) Bridge buy.
(4) Organic industrial base design and manufacturing.
(5) Reverse engineering for key components at risk of obsolescence/counterfeiting.
(6) Redesign of items to eliminate the key components or parts and materials at risk of obsolescence/counterfeiting.
(7) Substitutions of key components or parts and materials at risk of obsolescence/counterfeiting.
(8) Additive manufacturing.

3–10. Supply chain

a. Traceability. Any unauthorized supplier of parts, components, and parts and materials will provide a Certificate of Conformance showing traceability to all the supply chain intermediaries, from the actual manufacturer to the ultimate supplier. The Certificate of Conformance will include manufacturer's names and address, manufacturer's part number, the quantity of items purchased, lots and date codes (DCs), and customer shipping information.

b. Ordering procedures.

(1) Whenever possible, all parts and material will be ordered through approved government systems to reduce the risk for counterfeit. The use of credit card purchases from an unproven source adds considerable risk to the supply chain and will only be used as a last resort.

(2) Long lead time items can cause delays and often lead DoD supply chain members to look to nonauthorized suppliers who can provide a shorter lead time. This significantly increases the risk of counterfeit entering the supply chain. Therefore, parts and material are to be proactively managed and ordered to minimize unexpected delays due to long lead times.

c. Counterfeit Electronic and Non-Electronics Parts Management Plan. Army organizations will develop and implement a counterfeit parts control plan that documents processes for counterfeit prevention, risk mitigation, disposition, and reporting of suspect and confirmed counterfeit parts. A general Parts Management Plan Development Guide can be found in MIL–STD–3018, and guidance for developing an Electronic Components Management Plan is available in SAE EIA–STD–4899.

d. Parts and material control. All suspect counterfeit parts will be strictly controlled and not disposed of until provided guidance by U.S. Army legal authority. Even in the event of a refund, suspect counterfeit parts and materials will not be returned to the supplier. Suspect counterfeit parts and materials must be quarantined and disposed of so they cannot re-enter the supply chain.

Chapter 4
Reporting

4–1. Overview

Reporting and communicating the latest suspect and confirmed counterfeit parts and materials in the Army's supply chain is essential to maintain operational performance of equipment and preserve the life and safety of operating personnel. Investigative organizations, intelligence authorities, and all users of the counterfeit or suspect counterfeit parts and materials will be notified at the earliest opportunity. When the parts and materials identified as counterfeit or suspect counterfeit are critical, notification within the Army and to other DoD components will be expedited.

4–2. Reporting sources

a. Government-Industry Data Exchange Program. The GIDEP is to be used for reporting all suspected counterfeit parts and materials per DoDI 4140.67 and DFARS 252.246–7007. This cooperative activity between government and industry participants seeks to share essential technical information during all life cycle phases of the items. The web page link for GIDEP is listed in table 4–1. Reports must be entered into GIDEP within 60 days of awareness per FAR 46.317 and 52.246–26.

b. Product Data Reporting and Evaluation Program system of record. The PDREP is to be used as the reporting system of record per AR 702–7/DLAR 4155.24/SECNAVINST 4855.5B/AF Technical Order 00–35D–54/DCMA INST 305 and AR 702–7–1. This Department of the Navy program supports requirements regarding the reporting, collection, and use of supplier performance information. The PDREP is a best practice DoD data repository for supplier data, which promotes continuous process improvement for increased parts and material readiness and decreased deficiency issues, providing overall cost savings to the DoD. The web page link for PDREP is listed in table 4–1. Reports are to be entered as soon as practically possible, but no later than 60 days from the time of discovery per FAR 46.317 and 52.246–26.

4–3. Investigation resource

Investigations to determine criminal liability are conducted on a case-by-case basis. All cases will be reported to investigative and intelligence authorities for their review and decision. The decision to investigate usually depends on if the parts and materials surpass a dollar value threshold or is critical to the safety or functionality of the end item system, but each case is unique. The U.S. Army Criminal Investigation Division (USACID) and the U.S. Army Military Intelligence (MI) both have personnel who investigate potential counterfeit threats against U.S. Army equipment. Additional support for identifying and contacting regional USACID and MI representatives can be found in table 4–1.

Table 4–1
Reporting and investigation resources—Con

Source	Web page
Counterfeit Prevention Portal	https://ibwebportal.ria.army.mil/cpp/
GIDEP	https://www.gidep.org
PDREP	https://www.pdrep.csd.disa.mil/

4–4. Process

The steps in this paragraph provide a standardized methodology and process that can be used across the Army enterprise for reporting and communicating information on both suspected and confirmed counterfeit parts and materials.

a. Upon determination of suspect counterfeit, all parts and materials will be impounded, including parts and material from the same lot and DC. This includes uninstalled (stock on shelf and on the production floor) parts and material, in-process or finished subassemblies and assemblies, and installed parts and material in the field. Notify the program office, contracting officer, USACID, U.S. Army Materiel Command logistics assistance representative, Life Cycle Management Command, and materiel developer of the suspected counterfeit parts and material.

b. Report counterfeit and suspect counterfeit parts and material by filing an SF 368 (Product Quality Deficiency Report (PQDR)) in PDREP. When completing the PQDR, ensure that under the Detailed Cause Code answer the question “DO YOU SUSPECT THIS MATERIAL TO BE COUNTERFEIT?” by clicking “YES.” Based on this input, PDREP will automatically select “5AS–COUNTERFEIT MATERIEL, SUSPECT.”

c. File a GIDEP report within 60 days of identifying counterfeit and suspect counterfeit items, unless otherwise instructed by investigative authorities. Notify other DoD components to maintain weapons systems operational performance and preserve life or safety of operating personnel.

d. Upon request, provide parts and materials to investigative authorities and legal to support ongoing investigations and/or prosecution. Do not dispose of suspect or confirmed counterfeit parts and materials without approval from investigative authorities, legal, and the contracting officer.

e. Update reports in PDREP and GIDEP in accordance with the results of additional testing and investigation per AR 702–7/DLAR 4155.24/SECNAVINST 4855.5B/AF Technical Order 00–35D–54/DCMA INST 305 or AR 702–7–1.

Chapter 5
Physical Inspection and Testing

Section I

General

5–1. Overview
The physical inspection process is critical in preventing the purchasing and use of counterfeit parts and materials. Basic detection techniques are to be employed for any parts and material received or procured for use in government systems. Further testing will be determined by the program office based on the criticality and risk of the item and supplier and documented in a detailed test plan to include specific tests. For high-risk, critical, and safety items, testing will take place before the items are introduced into the supply chain.

5–2. Risk management
High-risk parts and material requires the most frequent and stringent tests. These items can be critical function components, safety items, or parts and materials that are at a high risk of counterfeiting, such as electronics, software, embedded memory, and/or communications technology equipment. A counterfeit detection test will be carried out on all such items prior to integrating them into higher level assemblies. A considerable risk is also present for parts and materials that were purchased before there was significant awareness of counterfeit risk. There is the potential that some of these parts and material were purchased from unauthorized suppliers and placed into the stockroom with no authentication performed. It is important to maintain stock control/traceability in stocks in order to attempt to identify and authenticate older parts and material.

a. Place focus on safety items and items with a high risk of being counterfeit such as electronics or items in obsolescence.

b. Develop a planned method or procedure for the authentication of high-risk critical parts and material procured from high-risk suppliers.

c. 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 standards SAE AS5553, SAE AS6081, and SAE AS6171 provide a suite of tests that can be used to detect counterfeit electronic parts. These tests are to be documented in an individualized test plan for the item or part.

d. In cases of item obsolescence, more high-risk suppliers are in the market and the OEM or authorized suppliers may have left the market. Parts and material is more likely to have been stored for a longer period of time and may have changed hands multiple times. The handling and storage processes increase the likelihood the parts and material is no longer in OEM/OCM condition. Considerable risk also occurs as items that may have been recycled back into the supply chain.

Section II

Inspection

5–3. Onsite inspection
Onsite inspection will be conducted at the location of item receipt by personnel on the material and/or parts as well as any corresponding packaging and documentation. During the inspection process, it is not uncommon for minor counterfeit indicators to be identified. These minor indicators, such as scratches or smudges, can occur in production or handling and are not a reliable indicator of counterfeit on their own. Further inspection and testing will be conducted to identify counterfeit parts and material.

5–4. Documentation inspection

The initial checkpoint in the identification of counterfeit parts and material is the inspection of all paperwork, packaging, and part labels that accompany the shipment. Documentation is often forged with counterfeit parts and materials and will be examined upon arrival for inconsistency between the purchase order and provided documentation.

a. Depending on the parts and material, the documentation will include:

(1) Certificate of Conformance.

(2) Shipment origin location.

(3) Special testing or screening certification.

(4) Manufacturer or supplier performed testing (assurance).

(5) Supply chain management/inventory data such as DCs, lot codes, quantity, and so forth.

b. The inspection should focus on missing or suspicious items such as misspelled words, inaccurate logos, inaccurate bar codes, poor grammar, and so forth.

(1) *Documentation.* Typical identification of risk types includes:

(a) Excessively faded, unclear, or missing data.

(b) Uneven/inconsistent type style, size, or pitch change.

(c) Data on a single line is located at different heights.

(d) Cut and paste appearance of paperwork.

(e) Mixed content such as typed and handwritten.

(f) Corrections are not properly lined-out, initialed, and dated.

(g) Document data is not legible, is mismatched, or/and missing.

(2) *Certification.* Typical identification of risk types includes:

(a) Technical data is inconsistent.

(b) Identical certification/test results; some variation in authentic test results are natural and should be expected.

(c) Certificate of Conformance and testing is not delivered as required.

(d) No item traceability.

5–5. Item and/or parts and material inspection

Some indicators provide a high level of confidence that the parts and material may be counterfeit (for example, discrepancies in logo design in the same package, nonmagnetic parts and materials attracted to a magnet), while other indicators (smudges, chips, and scratches) might be a result of processing, handling, or other processes which can be, but are not always, counterfeit indicators. See appendix B for additional indicators of counterfeit electronic parts. Care must be taken to perform enough authentication work to determine authenticity with a reasonable level of confidence. Two initial steps that must occur when reviewing for authenticity are: identify multiple suspect counterfeit indicators and obtain information from the OEM/OCM to support the suspicion that the part is counterfeit.

a. Indicators can be grouped by their significance to determine the level of risk. The levels of indicators include:

(1) Minor indicator. Sign of processing, quality, or handling which may or may not be related to counterfeiting such as documentation errors or scratches and other marks.

(2) Moderate indicator. Cause of suspicion for the part's authenticity such as multiple DCs in the same package or marking on part that does not match packaging documentation.

(3) Major indicator. Strong risk that the part has been modified and qualifies as counterfeit, such as part surfaces appearing recoated or mismatched logo or part numbers within a lot.

b. If a major indicator appears, or multiple moderate and minor indicators appear, quarantine the parts until further examinations can be conducted. A PDREP and GIDEP report for suspect counterfeit must be written and completed once further testing occurs.

Section III

Testing

5–6. Test facilities

Government laboratory test facilities will be used to conduct testing, unless the testing requirements are not available in the government facilities. If no government testing capabilities exist, then certified

commercial laboratory testing facilities will be utilized. Regardless of the source of testing, the following criteria are to be used when selecting a test laboratory:

a. Laboratory is an International Organization for Standardization (ISO)-compliant organization with a quality assurance program, trained personnel, and proof of responsibilities.

b. Examples of best laboratory practices include validated test plans and methodologies for the particular parts and parts and materials requiring testing with proof of calibrated test equipment.

c. Standardized and documented procedures to support testing, storage, data compiling process and archival includes storage of records and reports.

5–7. Assurance and authentication organizations

a. Joint Federated Assurance Center. Software and Hardware Assurance Joint Federated Assurance Center (JFAC) is a federation of DoD organizations that promotes and enables software assurance (SwA) and hardware assurance (HwA). The JFAC member organizations and their technical service providers interact with program offices and other interested parties to provide SwA/HwA expertise and support, to include vulnerability assessment, detection, analysis and remediation services, information about emerging threats and capabilities, software and hardware assessment tools and services, and best practices. The objectives are:

(1) Support program offices by identifying and facilitating access to DoD SwA and HwA expertise and capabilities to reduce vulnerabilities in fielded DoD systems.

(2) Assess capability gaps over time and recommend plans to close gaps.

(3) Develop recommendations for initiatives in support of the DoD research and development strategy to innovate vulnerability analysis, testing, and protection tools for SwA and HwA.

(4) Serve as the DoD POC for SwA and HwA interdepartmental and interagency efforts.

(5) Develop and sustain a department inventory of SwA and HwA resources, including tool licenses.

b. Defense Logistics Agency.

(1) DLA authenticates certain high-risk parts. This part population encompasses Federal Stock Class (FSC) category 5962 (electronic microcircuits). DLA's process provides marking of all parts with a DNA-based ink that fluoresces under examination by ultraviolet light. This marking signifies the parts were bought from an authorized supplier or that adequate authentication analysis has been performed. All electronic microcircuit parts purchased from DLA will be checked to ensure the DLA ink marking is present. DLA recommends inspecting to package requirements and completing a 100 percent visual inspection per SAE AS6081. Failure to detect this ink might be an indicator that the parts were procured by DLA before enactment of this marking and that these parts must be authenticated if DLA purchased them from outside the authorized supply chain.

(2) 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 (semiconductor devices and associated hardware) and FSC 5962 (microcircuits, electronic). DLA has QSLD listings for other parts and material as well, including mechanical parts.

(3) DLA also maintains a Qualified Testing Suppliers List (QTSL), which establishes QMS and inspection/test requirements for FSC 5961 and FSC 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.

5–8. Suspected counterfeit parts and parts and materials

a. Initial containment. Suspected counterfeit parts and materials will be segregated in a controlled access area at all times to ensure the parts and materials do not re-enter the inventory.

(1) *Segregation.* When the product is being tested, the entire lot must be segregated from all other similar parts and material in a secured location. This will ensure that no product is mistakenly recorded as a different item or sent to approved stock as acceptable inventory prior to completion of testing.

(2) *Data record.* The source of testing will be required to provide a report of testing performed to include appropriate pictures of product prior to and after testing. The report must include the tests conducted, the sample size tested, results obtained, and determination of findings regarding the item's authenticity. This data will be stored in a standardized format and retrievable for future reference.

(3) *Impounding.* Suspect counterfeit parts and material will be impounded with other items from the same lot and DC. This includes uninstalled parts and material, as well as in-process assemblies, installed

hardware, and finished assemblies. Product shipments to the customer for further processing or installation will be traced and impounded.

b. Additional counterfeit parts and material.

(1) The containment process must determine the possibility of additional counterfeit parts and material by investigating prior purchases of parts and material from the supplier or authorized distributor.

(2) All potential items with the suspect parts and material will be traced and both the program office and users will be notified of the potential issue.

Chapter 6
Disposition

6–1. Overview

Once suspect and confirmed counterfeit parts and materials have been identified, quarantined, investigated, and reported, they still must be properly disposed of to fully mitigate the threat posed to the warfighter. If counterfeit parts and materials are returned to the supplier for a refund, the parts and materials gain a second opportunity to enter the DoD supply chain through a purchase by a separate DoD entity. Parts and materials can also re-enter the supply chain through recycling programs, allowing a supplier to present and sell used parts and materials as brand new. To prevent these reintroductions of used and counterfeit parts and materials back into the supply chain, all counterfeit parts and materials and end of service life items must be mutilated beyond use prior to disposing or recycling.

6–2. Reissuance risks

Recycling and reissuance of parts and materials that are suspected counterfeit, confirmed counterfeit, and parts and materials that have been used to the end of its useful service life introduce a risk to warfighter safety and mission success if not properly disposed.

a. Counterfeit parts and material that are returned to the supplier can be resold to other U.S. military agencies and reintroduced into the DoD supply chain.

b. Parts and materials that have reached their end of service life are at risk of being recycled, refurbished, and sold as new to users in the DoD.

c. Specialized equipment for creation of military specific parts will be disposed of properly. Failure to properly dispose of specialized manufacturing equipment could result in the equipment being recycled and unauthorized manufacturers producing and selling counterfeit parts and materials.

6–3. Process

While some items have specific disposal and demilitarization instructions, many components do not. This paragraph provides a standardized set of instructions for disposal of suspected and confirmed counterfeit parts and materials, to be followed in conjunction with any published item-specific disposal instructions and in consultation with the item manager.

a. Impound all parts and materials with the same lot and DC as suspect counterfeit parts and material. Mark all impounded parts and materials as “Suspect Counterfeit” and quarantine so they cannot be unintentionally used or installed on a higher level assembly.

b. Trace back all locations the parts and materials have been since they entered the supply chain to ensure all parts and materials were accounted for in the initial quarantine.

c. Do not return parts and material to supplier, even if it means loss of reimbursement cost.

d. Provide any requested parts and materials to investigators/legal to support potential prosecution. Do not dispose of suspect or confirmed counterfeit parts and materials without approval from investigative authorities, legal, and the contracting officer.

e. Upon disposal authorization, parts and materials must be destroyed beyond use so they cannot re-enter the supply chain. Properly destroy or mutilate counterfeit parts and materials in accordance with DoDM 4160.21 Volume 1, which states that parts and materials classified as counterfeit “must be mutilated by the generating activity according to specific instructions provided by the item manager.” Mutilation methods 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. Do not put parts and material into the recycling stream unless it has been rendered completely inoperable for any use.

f. If unsure of proper disposition method, contact DLA Disposition Services for guidance and disposal as the office is familiar with the strict record keeping and procedures required for handling and disposing counterfeit parts and materials. Ensure that the proper label, usually “Property: Suspected Counterfeit,” is used when shipping counterfeit parts and materials to DLA Disposition Services to maintain quarantine of the parts and materials.

Appendix A

References

Section I

Required Publications

Unless otherwise indicated, DA publications are available on the Army Publishing Directorate website at https://armypubs.army.mil/. DFARS is available at https://www.acquisition.gov/dfars. DoD publications are available on the Executive Services Directorate website at https://www.esd.whs.mil/dd/. The FAR is available at https://www.acquisition.gov/browse/index/far. SAE standards are available for purchase at https://www.sae.org/standards.

AR 702–20
Counterfeit Risk Management Product Assurance (Cited in para 1–1.)

AR 702–7/DLAR 4155.24/SECNAVINST 4855.5B/AF Technical Order 00–35D–54/DCMA INST 305
Product Quality Deficiency Report Program (Joint Service Regulation) (Cited in *para 4–2b*.)

AR 702–7–1
Reporting of Product Quality Deficiencies within the U.S. Army (Cited in *para 4–2b*.)

DFARS 246.870
Contractors' Counterfeit Electronic Part Detection and Avoidance (Cited in *para 3–5a*.)

DFARS 252.246–7007
Contractor Counterfeit Electronic Part Detection and Avoidance System (Cited in *para 4–2a*.)

DFARS 252.246–7008
Sources of Electronic Parts (Cited in *para 3–5c*.)

DoDI 4140.01
DoD Supply Chain Materiel Management Policy (Cited in para 3–8.)

DoDI 4140.67
DoD Counterfeit Prevention Policy (Cited in *para 4–2a*.)

DoDI 5000.02
Operation of the Adaptive Acquisition Framework (Cited in *para 3–2a*.)

DoDI 5200.44
Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) (Cited in *para 3–2a*.)

DoDI 7050.05
Coordination of Remedies for Fraud and Corruption Related to Procurement Activities (Cited in para 2–2b(8).)

DoDM 4160.21 Volume 1
Defense Materiel Disposition: Disposal Guidance and Procedures (Cited in *para 6–3e*.)

FAR Part 46
Quality Assurance (Cited in para 2–2b(8).)

FAR 46.317
Reporting Nonconforming Items (Cited in *para 4–2a*.)

IDEA–STD–1010
Acceptability of Electronic Components Distributed in the Open Market (Available for purchase at https://www.idofea.org/idea-std-1010-inspection-standard.html.) (Cited in *para 3–9d*.)

MIL–STD–3018
Parts Management (Available at https://quicksearch.dla.mil/qssearch.aspx.) (Cited in *para 3–10c*.)

SAE AS5553
Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition (Cited in *para 3–9c*.)

SAE AS6081
Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition—Distributors (Cited in *para 3–9d*.)

SAE AS6171
Test Methods Standard; General Requirements, Suspect/Counterfeit, Electrical, Electronic, and Electromechanical Parts (Cited in *para 3–9d*.)

SAE AS6171/1
Suspect/Counterfeit Test Evaluation Method (Cited in *para 3–9d*.)

SAE AS6174
Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel (Cited in *para 3–9c*.)

SAE AS6496
Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition—Authorized/Franchised Distribution (Cited in table E–1.)

SAE EIA–STD–4899
Requirements for an Electronic Components Management Plan (Cited in *para 3–10c*.)

Section II

Prescribed Forms
This section contains no entries.

Appendix B

Quality Assurance for Parts and Materials

This appendix provides steps and instructions to assist with prevention and detection of counterfeit parts and material in the supply chain.

B–1. Assessment of contractor reliability to determine counterfeit risk

Any question in table B–1 that can be answered "no" indicates a risk indicator. For any question that does not apply, include contractual requirements, industry standards, or internal (contractor specific) guidance documents.

Table B–1
Assessment of contractor reliability to determine counterfeit risk

Item	Does the contractor have documented policies and procedures in place that address a minimum of:
1	Anti-counterfeit personnel training?
2	Inspection and testing of parts, with set acceptance and rejection criteria?
3	Quarantining and reporting counterfeit parts and suspect counterfeit parts?
4	Abolishing counterfeit parts proliferation and preventing their return to the supply chain?
5	Risk-based tracking of part traceability from original manufacturer to product acceptance by the Government?
	a. For discrete parts?
	b. For parts contained in assemblies?
	c. If traceability from the original manufacturer cannot be established, is the contractor responsible for inspection, testing, and authentication in accordance with applicable industry standards?
6	Does the contractor maintain documentation of:
	a. Traceability from original manufacturer to product acceptance by Government?
	b. Inspection, testing, and authentication when traceability cannot be established?
	c. Does the contractor provide this documentation to the Government upon request?
7	Contractor source of supply?
	a. Original manufacturer?
	b. AAM?
	c. Contractor-approved supplier?
	(1) Does the contractor ensure that contractor-approved suppliers utilize established counterfeit prevention industry standards?
	d. Other than contractor-approved supplier?
	(1) Does the contractor notify the contracting officer in writing?
	(2) Does the contractor utilize established counterfeit prevention industry standards to obtain the part?
8	Identification of suspect parts?
	a. Methodologies to rapidly verify if suspect part is counterfeit?
9	Systems are designed, operated, and maintained to detect and avoid suspect and counterfeit parts?
10	Require flow-down of counterfeit detection and avoidance policies to all subcontractors in the supply chain?
	a. Those responsible for buying or selling parts or assemblies?
	b. Those responsible for performing authentication testing?
11	Stay informed of current counterfeit information and trends?
	a. Screens GIDEP reports and other credible sources of counterfeit information to avoid the purchase and/or use of suspect and counterfeit parts?
12	Maintain control of obsolete parts to maximize availability and use of authentic, originally designed, and qualified parts throughout the product's life cycle?
13	Effective management of lead time in procurement planning to preclude need for using unauthorized sources, and maximize procurements through authorized sources?

B–2. Detection of counterfeit or suspect counterfeit parts upon receipt of parts and material

Each lot, batch, or DC should be authenticated as a separate authentication lot. An authentication lot is defined as one shipment of a specific lot, DC, batch number, or other group identification.

a. Section 1 of table B–2 is to be completed for all incoming parts and material.

(1) *Inspection of documentation.* Answers of "Yes" for any line items under 1g, 1h, or 1i are risk indicators.

(2) *Visual inspection.* Answers of "Yes" for line items 2 or 3 are risk indicators.

b. Section 2 of table B–1 is to be completed for parts and material that are not purchased from OCM/OEM or authorized supplier, and are critical parts and material known to be susceptible to counterfeiting.

(1) *Electronic parts.* Functional testing does not guarantee authenticity for electronic parts. The preferred standard for inspection and testing for electronic parts is SAE AS6081.

(2) *Mechanical parts.*

(a) There is no core set of inspections and tests that are applicable for all mechanical parts and materials. The standard of avoiding and detecting counterfeit mechanical parts and materials is SAE AS6174.

(b) Line items 5b, 5c, and 5d list potential tests and equipment that can be used in counterfeit detection.

c. Section 3 of table B–1 is to be completed for parts and material that is suspect counterfeit.

Table B–2
Detection of counterfeit or suspect counterfeit parts upon receipt of parts and material

Section 1: For ALL incoming parts and material:	
Item	**Inspection type**
Initial documentation inspection	
1	Inspect all paperwork, including packaging and part labels, which accompanies the shipment. Missing or suspicious information can be based on previously received documentation for the same parts and material.
	Documentation should provide:
	a. Origin of the shipment.
	b. Certification of any special testing and/or screening.
	c. Any supplier performed authentication.
	d. DCs.
	e. Lot codes.
	f. Quantity.
	Categories of counterfeit documentation include:
	g. Altered documents.
	(1) Excessively faded, unclear, or missing data.
	(2) Use of correction fluid or tape.
	(3) Type size, style, or pitch change is evident.
	(4) Data on a single line is located at different heights.
	(5) Lines on forms are bent, broken, or interrupted (indicates data has been deleted or "cut and paste").
	(6) Handwritten entries on a document with typed or preprinted data.
	(7) Text on page ends abruptly.
	(8) Number of pages conflicts with the transmittal.
	(9) Other.
	h. Signatures and initials.
	i. Certification.
	(1) Technical data is inconsistent with code or standard requirements.

Table B–2
Detection of counterfeit or suspect counterfeit parts upon receipt of parts and material—Continued

	(2) Certification/test results are identical between all tested items (normal variation should be expected).
	(3) Documented certificate of conformance and testing is not delivered as required on the purchase order, or is in an unusual format.
	(4) Document is not traceable to the items procured.
	(5) Other.
Visual inspection	
2	Packaging.
	a. Mixed internal designs in same packaging, incorrect labels, and so forth.
3	Markings.
	a. Smudged markings, chips, scratches, and so forth.
Section 2: If critical parts and material known to be susceptible to counterfeiting, and NOT purchased from OCM/OEM or authorized supplier.	
Parts and material authenticity inspection/test	
4	Electronic parts.
	a. SAE AS6081.
5	Mechanical parts and materials (there is no core set of techniques across the board; below are examples of equipment and test methods that are useful).
	a. SAE AS6174.
	b. Parts and material visualization and measurement.
	(1) Stereo microscope.
	(2) Optical microscope.
	(3) Digital microscope system.
	(4) Scanning electron microscopy.
	(5) Non-contact measurement system.
	(6) Contact coordinate measuring machine.
	(7) Profilometer.
	c. Alloy/material identification.
	(1) Scanning Electron Microscope-Energy Dispersive Spectroscopy (SEM–EDS).
	(2) X-Ray Fluorescence Spectroscopy (XRF).
	(3) Induction Coupled Plasma Atomic Emission Spectroscopy (ICP–AES).
	(4) Fourier Transform Infrared Spectroscopy (FTIR).
	(5) X-Ray Photoelectron Spectroscopy (XPS).
	d. Heat-treatment/finish identification.
	(1) Mechanical cross-section grinding and polishing.
	(2) Chemical and thermal etching of microstructure.
	(3) Rockwell hardness, scales A, B, C, D, and superficial.
	(4) Micro hardness, Knoop and Vickers.
Section 3: If parts and material are suspect.	
Methods to confirm counterfeit	
6	Quarantine parts and material.
7	Document multiple indicators that the parts and material are counterfeit.

Table B–2
Detection of counterfeit or suspect counterfeit parts upon receipt of parts and material—Continued

8	Obtain the OCM/OEM analysis and response that the parts and material are likely counterfeit.
9	Report to program office, PDREP, GIDEP, and so forth.
	a. Corrections not properly lined-out, initialed, and dated.
	b. Document is not signed or initialed where required.
	c. The name or title of the document approver cannot be determined.
	d. Approver's name and signature do not match.
	e. Document has missing or illegible signature or initials.
	f. Other.

B–3. Indicators of counterfeit parts

Tables B–3 and B–4 provide guides to assess the strength of a counterfeit indicator.

Table B–3
Indicators of counterfeit electronic parts

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 OCM/OEM 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 OCM/OEM Logo on box/tube/tray/reel	Major
	Not in original manufacturer's packaging	Minor
	Use of non-electro static discharge protected material	Moderate
	Not in a sealed moisture barrier bag	Minor
	Humidity indicator card 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 or DC in documentation	Moderate
	Mismatch in part quantity in documentation	Minor
	Erroneous OCM/OEM Logo on documents	Major
	Evidence of tampering in documentation	Moderate
Part Marking/Identification Inspection	Three or more DCs 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

Table B–3
Indicators of counterfeit electronic parts—Continued

Test Type	Counterfeit Indicator	Strength of Indicator
	Inconsistent part indentation (for example, pin 1), top or bottom	Major
	Inconsistent country of origin information	Major
	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, and so forth.)	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 surface cleaner or alcohol	Moderate
	Surface coating is removed by surface cleaner alcohol	Major
	Hidden “ghosted” markings uncovered by surface cleaner alcohol	Major
	Internal die or wirebonds exposed by surface cleaner or alcohol	Major
	Sanding underneath surface uncovered by surface cleaner or alcohol	Major
Surface Scrape	Surface coating is removed by a razor knife	Major

Table B–3
Indicators of counterfeit electronic parts—Continued

Test Type	Counterfeit Indicator	Strength of Indicator
	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
	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 material	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 within scan	Minor
	Inconsistent die size or design on parts in same lot	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 (for example, traces, spacing, contamination, and so forth.)	Minor
	Wrong OCM/OEM or logo	Major
	Mismatched part number	Minor
	Incorrect wire bond material	Major
	Inconsistent OCM/OEM 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

Table B–3
Indicators of counterfeit electronic parts—Continued

Test Type	Counterfeit Indicator	Strength of Indicator
	Impossible DC (die year after part)	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
	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/DC format	Moderate
	Unmatched lead design	Moderate
	Unmatched lead frame	Minor
	Unmatched die markings	Minor
OCM/OEM Support	Component manufacturer states parts are likely counterfeit	Major
	Component manufacturer states parts are possibly counterfeit	Moderate

Table B–4
Indicators of counterfeit mechanical parts and materials·

Test/Material 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 Universal Product Code (UPC)	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 OCM/OEM 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

Table B–4
Indicators of counterfeit mechanical parts and materials—Continued

Test/Material Type	Counterfeit Indicator	Strength of Indicator
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
Documentation Indicators	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, and so forth)	Pitting or corrosion	Moderate
	External weld or heat indications	Major
	Questionable or meaningless numbers	Major
	Typed labels	Moderate
	Evidence of handmade 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

Table B–4
Indicators of counterfeit mechanical parts and materials—Continued

Test/Material Type	Counterfeit Indicator	Strength of Indicator
	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
	Some parts (for examplee, hand wheels) look newer than the rest of the valve	Minor
	Excessive or missing markings (for example, 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, and so forth	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/DC	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

Appendix C

Federal Supply Group Counterfeit Risk Lists

C–1. High-risk items

Table C–1 provides a list of items identified by DLA as high counterfeit risk.

Table C–1
High-risk counterfeit items—Cc

FSG Number	FSG Title
10	Weapons
12	Fire Control Equipment
15	Aircraft and Airframe Structural Components
16	Aircraft Components and Accessories
17	Aircraft Launching, Landing, and Ground Handling Equipment
20	Ship and Marine Equipment
25	Vehicular Equipment Components
28	Engines, Turbines, and Components
29	Engine Accessories
30	Mechanical Power Transmission Equipment
31	Bearings
40	Rope, Cable, Chain, and Fittings
43	Pumps and Compressors
47	Pipe, Tubing, Hose, and Fittings
48	Valves
53	Hardware and Abrasives
55	Lumber, Millwork, Plywood, and Veneer
59	Electrical and Electronic Equipment Components
61	Electric Wire, and Power and Distribution Equipment
66	Instruments and Laboratory Equipment
70	Automatic Data Processing Equipment (Including Firmware), Software, Supplies, and Support Equipment
89	Subsistence

C–2. Medium-risk items

Table C–2 provides a list of items identified by DLA as medium counterfeit risk.

Table C–2
Medium-risk counterfeit items—Cc

FSG Number	FSG Title
14	Guided Missiles
26	Tires and Tubes
36	Special Industry Machinery
37	Agricultural Machinery and Equipment
38	Construction, Mining, Excavating, and Highway Maintenance Equipment
39	Materials Handling Equipment
41	Refrigeration, Air Conditioning, and Air Circulating Equipment
42	Fire Fighting, Rescue, and Safety Equipment; and Environmental Protection Equipment and Materials
45	Plumbing, Heating, and Waste Disposal Equipment

Table C–2
Medium-risk counterfeit items—Continued

FSG Number	FSG Title
49	Maintenance and Repair Shop Equipment
51	Hand Tools
52	Measuring Tools
56	Construction and Building Materials
58	Communication, Detection, and Coherent Radiation Equipment
60	Fiber Optics Materials, Components, Assemblies, and Accessories
62	Lighting Fixtures and Lamps
63	Alarm, Signal, and Security Detection Systems
65	Medical, Dental, and Veterinary Equipment and Supplies
67	Photographic Equipment
68	Chemicals and Chemical Products
71	Furniture
72	Household and Commercial Furnishings and Appliances
73	Food Preparation and Serving Equipment
74	Office Machines, Text Processing Systems and Visible Record Equipment
75	Office Supplies and Devices
76	Books, Maps, and Other Publications
77	Musical Instruments, Phonographs, and Home-Type Radios
80	Brushes, Paints, Sealers, and Adhesives
81	Containers, Packaging, and Packing Supplies
83	Textiles, Leather, Furs, Apparel and Shoe Findings, Tents and Flags
84	Clothing, Individual Equipment, and Insignia
91	Fuels, Lubricants, Oils, and Waxes
93	Nonmetallic Fabricated Materials
94	Nonmetallic Crude Materials
95	Metal Bars, Sheets, and Shapes
96	Ores, Minerals, and Their Primary Products
99	Miscellaneous

C–3. Low-risk items

Table C–3 provides a list of items identified by DLA as low counterfeit risk.

Table C–3
Low-risk counterfeit items—C

FSG Number	FSG Title
22	Railway Equipment
24	Tractors
32	Woodworking Machinery and Equipment
34	Metalworking Machinery
35	Service and Trade Equipment
44	Furnace, Steam Plant, and Drying Equipment; and Nuclear Reactors
46	Water Purification and Sewage Treatment Equipment
54	Prefabricated Structures and Scaffolding
69	Training Aids and Devices

Table C–3
Low-risk counterfeit items—Continued

FSG Number	FSG Title
88	Live Animals

C–4. Items not assessed

Table C–4 provides a list of items not assessed for counterfeit risk by DLA.

Table C–4
Items not assessed for counterfeit risk—Con

FSG Number	FSG Title
11	Nuclear Ordnance
13	Ammunition and Explosives
18	Space Vehicles
19	Ships, Small Craft, Pontoons, and Floating Docks
23	Ground Effect Vehicles, Motor Vehicles, Trailers, and Cycles
78	Recreational and Athletic Equipment
79	Cleaning Equipment and Supplies
85	Toiletries
87	Agricultural Supplies

Appendix D

Assessments to be Used in Support of AR 702–20

D–1. Industrial base technology capability assessment

At a minimum, all the questions in each section of table D–1 should be addressed in the assessment.

Table D–1
Industrial base technology capability assessment

Section 1: Assessment of Potential Industrial Sectors of the Technology **Purpose**: Identify current risk trends and potential risk sources related to the technology being considered for design into the material solution. **To Be Completed**: Pre-Milestone A.	
1	What is the probability of the proposed technology being counterfeited?
2	What are the current shortfalls in the trusted industry sectors?
3	What percent of suppliers are first-time sources of supply?
4	Is the proposed technology dependent on sources which could experience a shift in social economic posture?
5	Are there sources in countries which are identified as having less than favored nation status?
6	Has counterfeit prevention language been incorporated in the program of record's LCSP?
Section 2: Technology Availability Assessment **Purpose**: Support selection of the best materials to be used in the design of the material solution based on the future availability of the materials. **To Be Completed**: Milestone A.	
1	Long-term availability of material, to be completed for each finished material and any intermediate inputs.
	a. What is the stability of the supply chain for internal and external forces?
	b. What is the stability of the region where material is produced? For example, more volatile regions could face additional challenges in the delivery of material.
	c. Does the potential exist for insufficient access to intermediate inputs to the process, such as a lack of qualified personnel in the region, that could affect the supply chain?
	d. What is the financial health of the product line for the manufacturer? For example, a manufacturer will not continue to produce the material without continued demand, or if more financially lucrative products can be produced instead. This becomes crucial to parts that contain sole sourced materials.

D–2. Materiel developer counterfeit risk management assessment

At a minimum, all the questions in each section of table D–2 should be addressed in the assessment.

Table D–2
Materiel developer counterfeit risk management assessment—Continued

Section 1: Materiel Developer CRM Assessment **Purpose**: Support selection of the best materials to be used in the design of the material solution based on the future availability of the materials. **To Be Completed**: During the material selection process and included in the preliminary design review and all following systems engineering technical reviews	
1	Is there a technology roadmap of the parts and materials selected and the long-term availability of the parts and materials?
2	What is the stability of the suppliers and location (region) of the suppliers?
3	Are critical functionalities identified?
4	Are the criticalities of items and components defined?
5	Are critical application items identified?
6	Are susceptibility to counterfeiting certifications used for type classification are authorized for use in satisfying materiel release requirements when stated for dual use by the functional authority unless changes were made to the item? The type classification and materiel release processes ensure standard/full materiel release at full-rate production to verify the item is safe, suitable, and logistically supportable.

Table D–2 **Materiel developer counterfeit risk management assessment—Continued**	
7	Is the Risk Management Framework aligned, per DoDI 8510.01, which includes the appropriate methods, standards, and practices required to protect DoD information technology?
Section 2: Supplier Confidence Assessment **Purpose**: Determine supplier suitability if an unauthorized supplier is the only available source. The technical authority for the purchase will assess the unauthorized supplier prior to that supplier being considered a low risk supplier. **To Be Completed**: When an unauthorized supplier is the only available source.	
1	Has a parts and material source assessment been previously completed?
2	Has all paperwork, including packaging and part labels that accompanies the shipment, been inspected and compared to known authentic documentation (when available)?
3a	For electronic parts. Have they been inspected in accordance with SAE AS 6081?
3b	For mechanical parts and materials. There is no core set of techniques across the board for inspecting mechanical parts and materials. Have they been inspected using a combination of SAE AS6174, material visualization and measurement, alloy/material identification, heat-treatment/finish identification, or other method as applicable to the specific part?

Appendix E

Sample Language for Life-Cycle Sustainment Plan

E–1. Overview

The LCSP is part of life-cycle planning. Any new system must have information on how to mitigate the counterfeit risks in the parts and materials found in that system.

E–2. Sample plan

Table E–1 provides sample language to include in an LCSP.

Table E–1
Counterfeit Prevention Plan—Co…

Chapter [XX]–Counterfeit Prevention Plan	
	A counterfeit prevention plan shall be created that meets the requirements and prevention procedures provided in DoDI 4140.67, DoD Counterfeit Prevention Policy. This Counterfeit Prevention Plan (CPP) establishes a counterfeit prevention Product Assurance beginning no later than Acquisition Milestone A. The CPP is developed simultaneously into Milestone B and Milestone C as an integrated component of the LCSP. The CPP is also integrated into the Supply Chain Risk Management process and the System Engineering Plan to ensure commonality. The plan encompasses a risk assessment which considers the risk areas of: technology, sources of supply based on intelligence threats, vulnerability of the system, and components to counterfeit risk. Other risk considerations included in the plan are: (1) obsolescence, (2) cybersecurity, (3) market demands, both high and low which impact the likelihood of counterfeit entering the supply stream, and (4) historical trends utilizing North American Industry Classification System (NAICS). The CPP serves as a key performance indicator, which requires management to maintain a proactive plan across the entire system's life cycle in order to sustain system operational readiness. The LCSP CPP will be tailored to meet program needs through integration in maintenance and support concepts. The tailored CPP will: • Be addressed as an integral part of the program's acquisition strategy and system design process. • Assign responsibilities and management approach for achieving effective and timely acquisition, product support, and availability throughout the life cycle including the program manager's role in planning for and executing sustainment. • Include consideration for funding required to enable risk management. • Identify and select sources of repair or support. Appendix [XX] of the CPP template provides guidance for all component types within the system which ensures system component traceability, counterfeit detection, and avoidance.
Appendix [XX]	
Paragraph 1	1. DoDI Policy requirements. The [Supplier] and [Government agency] shall have an agreed upon “plan” and strategy in place to address counterfeit parts and materiel management of the supply chain risk. The plan shall meet all counterfeit prevention measures listed in DoDI 4140.67. The plan shall fulfill the requirements listed in the DoDI 4140.76.
Paragraph 2	2. SAE International Practices. The plan shall use anti-counterfeiting practices in accordance with Military Standards and SAE Standards, including but not limited to SAE AS5553, SAE AS6081, SAE AS6171, SAE AS6174, and SAE AS6496.
Paragraph 3	3. Materials. All components procured for a DoD system are to be genuine, reparable, and unused prior to assembly into the DoD system. This anti-counterfeit annex applies to every component of the DoD system, including but not limited to: all electrical components, electro-mechanical components, pneumatic components, raw materials, and common commodities.
Paragraph 4	4. Supply Chain Risk Management. Supply Chain Risk Management requirements shall be flowed down from [Supplier] to all sub-suppliers, with [Supplier] responsible for providing confirmation of counterfeit prevention plan and strategy. 4.1. Ordering Parts and Materiel. Supplier shall use new and authentic materials, commodities, items, assemblies, subassemblies, and components (collectively in this section “Materials”) in Goods. Supplier shall purchase materials directly from original equipment/component manufacturers, manufacturer authorized/franchised distributors, or authorized aftermarket manufacturers (collectively in this section “Sellers”) unless approved in advance by Buyer. Supplier, at the time of each individual Supplier quotation to a Seller, shall obtain from Seller: (i) the company name and location of the source of supply, and (ii) a representation that Seller is authorized to sell the Material.

Table E–1
Counterfeit Prevention Plan—Continued

	4.2. Traceability. Supplier shall maintain Material traceability including tracking of Materials to the Seller. Traceability shall also include: (i) the name and location of all of the supply chain intermediaries from the manufacturer to the direct source of the Materials for Supplier, and (ii) the manufacturer's commodity or item level identification for the item(s) such as date codes, lot codes, heat codes, serializations, unique item identifiers, or other batch identifications. 4.3. Obsolescence Risk. The risk of procuring counterfeit parts and materials significantly increases when an item becomes obsolete. As such, the plan shall work in conjunction with a plan on mitigating diminishing manufacturing sources and material shortages (DMSMS) to minimize the risk of obsolescence, thereby reducing the risk of counterfeit. 4.4. Risk Assessment. Items with high risks for counterfeit, notices of counterfeit from data sources previously identified, or critical to the safety and functionality of the system shall include risk mitigation steps for counterfeit avoidance in their plan. 4.5. Verification of materials. 4.5.1. Receiving Materials. Upon receipt, parts and materials shall be inspected within the original packaging, along with all accompanying certification documentation. The items will then be unpackaged and visually examined for indicators of item genuineness, in accordance with industry standards. Any order with items deemed suspicious of counterfeit shall be segregated in a controlled location to avoid unintentional re-entry into the supply chain. 4.5.2. Certificate of Conformance. Supplier shall approve, retain, and provide copies of Certificates of Conformance (CoC) which, at minimum, shall include the following: 4.5.2.1. Manufacturer name and address. 4.5.2.2. Manufacturer and/or Supplier’s part description, part number and dash number, group number, or similar. 4.5.2.3. Commodity or item level identification for the item(s) such as date codes, lot codes, heat codes, serializations, unique item identifiers, or other batch identifications. 4.5.2.4. Signature or stamp with title of seller’s authorized personnel signing the certificate. 4.5.3. Certificate of Authenticity. Supplier shall approve, retain, and provide copies of Certificates of Authenticity (CoA) which, at minimum, shall include the following: 4.5.3.1. Contract number. 4.5.3.2. Manufacturer name and address. 4.5.3.3. Manufacturer and/or buyer’s part number and dash number, group number or similar. 4.5.3.4. Item nomenclature, quantity, unit of measure. 4.5.3.5. Actual manufacturer CAGE code, design control activity CAGE code. 4.5.4. Test and Inspection. Supplier shall initiate and maintain test and inspection activities to assure the authenticity of materials, to include: supply chain traceability and documentation verification; visual examination; and applicable test and inspection activities. Supplier shall deliver to buyer records of tests and inspections performed and conformance of the material to specified acceptance criteria. Tests and inspections shall be performed by persons that have been trained and qualified concerning detection of the types and means of counterfeiting and how to conduct effective product authentication. 4.6. Disposal of Materials. Confirmed counterfeit parts and materials shall be destroyed in such a manner that they cannot re-enter the supply chain at any point in the future. The item shall not be destroyed until permission granted by a representative from the Program Office or the General Counsel’s Office Attorney assigned to the case. Disposal will take place at a qualified government facility. 4.7. Data Sources. Suppliers are to use appropriate counterfeit prevention and notification. At a minimum, every supplier and sub-supplier shall have access to the Government-Industry Data Exchange Program (GIDEP). This will be used for both counterfeit prevention and counterfeit notification. Commercial software may also be used to provide additional information and support on counterfeit prevention.

Table E–1
Counterfeit Prevention Plan—Continued

Paragraph 5	5. Reporting. All occurrences of suspected counterfeit parts and materials shall be reported to the assigned, onsite counterfeit Point of Contact (POC). The counterfeit POC is responsible to alert the Program Office, and General Counsel's Office. The POC will input information of the suspected counterfeit onto GIDEP and, if a government POC, Product Data Reporting and Evaluation Program (PDREP). If the item is of significant monetary value or critical to the safety of the system, the item is to be reported to the appropriate Defense Intelligence and/or Criminal Investigation Agency for review and potentially additional investigation. 5.1. Data sources. Suppliers are to use appropriate counterfeit prevention and notification. At a minimum, every supplier and sub-supplier shall have access to the GIDEP. This will be used for both counterfeit prevention and counterfeit notification. Commercial software may also be used to provide additional information and support on counterfeit prevention. 5.2. Government Data Sources URL. 5.2.1. GIDEP: https://www.gidep.org/. 5.2.2. PDREP: https://www.pdrep.csd.disa.mil/.
Paragraph 6	6. References. 6.1. DoDI 4140.67, DoD Counterfeit Prevention Policy, October 25, 2017. 6.2. DoDI 4140.01, DoD Supply Chain Materiel Management Policy, December 14, 2011. 6.3. MIL–STD–3018, Department of Defense, Standard Practice, Subject: Parts Management, June 2015. 6.4. Standard Document–19, Subject: Parts Management Guide, December 2013. 6.5. Office of the Assistant Secretary of Defense, Logistics and Materiel Readiness, Subject: Life-Cycle Sustainment Plan Outline Version 2.0, January 2017.

Glossary of Terms

Aftermarket manufacturer
A manufacturer that meets one or more of the following criteria:
a. The manufacturer is authorized by the OCM to produce and sell replacement parts, usually due to an OCM decision to discontinue production of a part. Parts supplied are produced from materials that have been transferred from the OCM to the aftermarket manufacturer, or produced by the aftermarket manufacturer using OCM tooling and intellectual property.
b. The manufacturer produces parts using semiconductor dice or wafers, manufactured by and traceable to an OCM, that have been properly stored until use and are subsequently assembled, tested, and qualified using processes that meet technical specifications without violating the OCM's intellectual property rights.
c. The manufacturer produces parts through emulation, reverse engineering, or redesign that match the OCM's specifications and satisfy customer needs without violating the OCM's intellectual property rights. In any case, the aftermarket manufacturer must label or otherwise identify its parts to ensure that the "as shipped" aftermarket manufactured part will not be mistaken for the part made by the OCM.

Approved supplier
Suppliers that are assessed and determined to provide acceptable fraudulent/counterfeit parts risk mitigation process.

Authorized supplier
See DFARS 252.246–7008(a).

Bill of materials
A listing of parts and required quantities; electronic, electrical, mechanical, and materials used to identify repair parts or parts need to fabricate (produce) a system or assembly.

Counterfeit electronic part
An unlawful or unauthorized reproduction, substitution, or alteration that has been knowingly mismarked, misidentified, or otherwise misrepresented to be an authentic, unmodified electronic part from the original manufacturer or a source with the express written authority of the original manufacturer or current design activity, including an AAM. Unlawful or unauthorized substitution includes used electronic parts represented as new, or the false identification of grade, serial number, lot number, DC, or performance characteristics.

Counterfeit material
See DoDI 4140.67.

Counterfeit part
A fraudulent part 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. A suspect part may be determined to be fraudulent or counterfeit through further evaluation and testing. All counterfeit parts are fraudulent, but not all fraudulent parts are counterfeit.

Critical component
See DoDI 5200.44.

Critical material
Includes critical components such as critical infrastructure information, critical application items and critical safety items, and other material identified by the cognizant service ESA prior to initial supportability analysis during the initial provisioning and cataloging or approval of a design change notice, and documented by the cognizant service logistics organization.

Critical safety item
See DoDI 4140.67.

Diminishing manufacturing sources and material shortages
The loss or impending loss of the last known manufacturer or supplier of raw materials, production parts, or repair parts.

Electronic part
See DFARS 252.246–7008(a).

Engineering support activity
See DoDI 4140.67.

Government-Industry Data Exchange Program
See DoDI 4140.67.

High risk
Material 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 material. Material often at high risk of counterfeiting includes ICs; discrete semiconductors (transistors, diodes, or optocouplers); high voltage, high value, or specialty (low equivalent series resistance (ESR), high quality, or trimmer) capacitors; mechanical roller bearings; specialty fasteners; lubricants; adhesives; batteries; and other materials identified in GIDEP or PDREP reports as susceptible to being counterfeited.

Item
A single hardware article or a single unit formed by a grouping of subassemblies, components, or constituent parts.

Life cycle
The life of an acquisition program consists of phases, each preceded by a milestone or decision point, during which a system goes through research, development, test, and evaluation; production; fielding or deployment; sustainment; and disposal. Currently, the five phases are materiel solution analysis, technology maturation and risk reduction, engineering and manufacturing development, production and deployment, and operations and support.

Manufacturer
An individual, company, corporation, firm, or government activity who controls the production of an item; or produces an item from crude or fabricated materials; or assembles materials or components or parts, with or without modification, into a more complex item.

Materiel
See DoDI 4140.67.

Part
See AR 750–1.

Product Data Reporting and Evaluation Program
The Department of the Navy program that supports requirements regarding the reporting, collection, and use of supplier performance information identified in the Code of Federal Regulations, FAR, DFARS, and Army regulations. PDREP supports Army management of the supply chain ensuring first time quality and on-time delivery of materials for both critical and noncritical applications.

Product quality deficiency report
PQDRs are used to determine the cause of discrepancies, effect corrective action, and prevent recurrences as required by the PQDR Program. PQDRs will be submitted for deficiencies detected on new or newly reworked government-owned products that do not fulfill their expected purpose, operation, or service due to deficiencies in design, specification, material, software, manufacturing process, and/or workmanship.

Product substitution
Substitution of a product or a component of a product that does not fully comply with all contract requirements. See DoDI 7050.05.

Program protection
The DoD's integrating process for mitigating and managing risks to advanced technology and mission-critical system functionality from foreign collection, design vulnerability, or supply chain exploitation/insertion, battlefield loss, and unauthorized or inadvertent disclosure throughout the acquisition life cycle.

Risk-based approach
See DoDI 4140.67.

Subcontractor
Any supplier, distributor, vendor, or firm that furnishes supplies or services to or for the contractor or another subcontractor under this contract.

Supply chain
See DoDI 4140.67.

Supply chain traceability
Documented evidence of a part's supply chain history. This refers to documentation of all supply chain intermediaries and significant handling transactions, such as from OCM to distributor, or from excess inventory to broker to distributor.

Suspect counterfeit
See DoDI 4140.67.

Traceability
See DoDI 4140.67.

Verification
The process for assessing the quality of a machine-readable symbol and assigning a grade to the results or otherwise indicating acceptance in accordance with the applicable specification or MRI protocol quality control document. Verification is performed using an electronic/optical verification device.

SUMMARY

DA PAM 702–20
Counterfeit Risk Management Product Assurance Handbook

This new Department of the Army pamphlet, dated 9 January 2023—

- Sets forth mandatory procedures to implement Army's counterfeit risk management product assurance as prescribed by AR 702–20 (throughout).

- Provides guidance for identifying suspect counterfeit parts and sample language for a Life-Cycle Sustainment Plan (apps B through E).