Headquarters
Department of the Army
Washington, DC
9 January 2023

Army Regulation 702–20

Effective 9 February 2023

Product Assurance

Counterfeit Risk Management Product Assurance

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 regulation.

Authorities. This regulation implements DoDI 4140.67.

Applicability. This regulation applies to the Regular Army, the 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 regulation 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.

Army internal control process. This regulation contains internal control provisions in accordance with AR 11–2 and identifies key internal controls that must be evaluated (see app B).

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

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

UNCLASSIFIED

Contents (Listed by chapter and page number)

Chapter 1
Introduction

Section I

General

1–1. Purpose
This regulation prescribes the Department of the Army (DA) policy for implementing the Army counterfeit risk management (CRM) product assurance, including assigning roles and responsibilities, and establishes policy for conducting anti-counterfeit activities in the execution of the Army CRM product assurance. This policy implements the CRM requirements, defining the process used to develop CRM within the Army's acquisition and sustainment processes and integrate CRM across the entire life cycle of the product. Guidance for implementing this policy is provided in DA Pam 702–20 and must be used in conjunction with this regulation.

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
Procedures associated with this regulation are found in DA Pam 702–20.

1–4. Responsibilities
See section II of this chapter.

1–5. 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.

1–6. Governance
This regulation governs all phases of parts and materials management, from identifying and defining an operational requirement to material or parts, to include commercial off-the-shelf (COTS) items being introduced into the supply chain, through weapon and information system phase-out and retirement, including operation and maintenance, disposition, and material management data systems, unless specifically stated otherwise.

Section II

Responsibilities
CRM is an Armywide responsibility from the lowest echelons to the highest, from the equipment operator and maintainer to the commander, and from the designer and logistician to the acquisition manager. The mission of the Army CRM product assurance is to enforce preventive CRM procedures that will reduce operational impacts to supply chain capabilities, supply availability, maintenance, and reliability in the sustainment of equipment readiness. To achieve this goal, conscious risk management processes must begin at the defense acquisition life cycle's material development phase (pre-acquisition Milestone A) and continue throughout the service life of a program. The end state objective is the construction and protection of resilient, responsive, and safe supply chains to sustain readiness.

1–7. Assistant Secretary of the Army (Acquisition, Logistics and Technology)
The ASA (ALT) exercises strategic management for the Army CRM product assurance and will—

a. Ensure CRM is maintained in all relevant policies and programs for Army acquisition, logistics, and technology initiatives under its purview.

b. In coordination with the Commanding Generals (CGs), Army Futures Command (AFC) and Army Materiel Command (AMC), plan, program, budget, and execute a research, development, test, and evaluation (RDT&E) program to investigate new and evolving technologies that can be used to support CRM within the Army.

c. When serving as the Headquarters, Department of the Army (HQDA) approval authority for a system engineering plan (SEP)/simplified acquisition management plan (SAMP), ensure that each SEP/SAMP reflects a risk-based approach to identify critical components or aspects of the system that can be threatened by counterfeit, as well as incorporates lessons learned from similar systems, to address CRM planning requirements in accordance with DoDI 4140.67.

d. Serve as the HQDA approval authority for a program protection plan (PPP) and ensure that each PPP reflects a risk-based approach to identify critical components or aspects of the system that can be threatened by counterfeit, as well as incorporates lessons learned from similar systems, to address CRM planning requirements in accordance with AR 70–77 and DoDI 5000.83.

e. As the HQDA Life Cycle Sustainment Plan (LCSP) approval authority, ensure that each LCSP reflects projected considerations from the risk-based approach used in the SEP/SAMP, as well as lessons learned from operational sustainment reviews of similar equipment, to address CRM planning requirements in accordance with AR 70–1, AR 700–127, DA Pam 700–127, DoDI 5000.02, and DoDI 5000.83.

f. Maintain and adequately resource the office of the Deputy Assistant Secretary of the Army for Sustainment to carry out the Title 10, United States Code (10 USC) statutory requirements and the responsibilities assigned in this regulation.

g. Through the Deputy Assistant Secretary of the Army for Sustainment, designate a DA Civilian to serve as the Army counterfeit risk management policy lead (CRMPL) who is responsible for overseeing DA-level CRM product assurance activities throughout the Army. The CRMPL will ensure that program executive officers (PEOs)—

(1) Oversee the materiel developers (MATDEVs) in performing their life cycle CRM planning requirements in accordance with DoDI 5000.02, DoDI 5000.83, AR 70–1, AR 700–127, AR 70–77, and DA Pam 700–127. This includes, but is not limited to, requirements in the SEP/SAMP, Test and Evaluation Master Plan, LCSP, and PPP; their risk-based approach to identify critical components and electronic parts; or aspects of systems that, when impacted by counterfeit, cause loss of capability or operability, decrease in safety, or increased resources for maintenance.

(2) Develop implementing guidance specific to the program managers (PMs) and MATDEVs in their commodity area on how to perform efficient and effective life cycle CRM planning in accordance with DoDI 5000.02, DoDI 5000.83, AR 70–1, AR 700–127, AR 70–77, and DA Pam 700–127. Review the guidance annually and provide copies to the Army CRMPL within 30 days of initial publication and revision.

(3) Evaluate the adequacy of PM and MATDEV CRM planning against the written guidance, internal controls in appendix B, and inform the Army CRMPL this was completed in a memorandum for record no later than than September 30th each year.

(4) Ensure all staff have an appropriate level of awareness and instruction on the CRM requirements and methods applicable for their duties and responsibilities.

(5) Ensure CRM requirements for SEP/SAMP, PPP, and LCSP are reviewed by Army CRMPL prior to initial publication and revision.

(6) Appoint a DA Civilian general schedule (GS)–13 equivalent (or above) or military equivalent to act as the primary CRM point of contact (POC) for their organization to the Army CRMPL within 60 days of promulgation of this regulation. Report the name and contact information to the Army CRMPL within 15 days of the appointment.

(7) Ensure that the primary CRM POC—

(a) Has appropriate technical background, duties, and responsibilities to carry out this function and the ability to collect and report annually on the required information.

(b) Provides timely, complete, and accurate information in response to all information requests distributed by the Army CRMPL, including but not limited to, annual reporting requirements, internal Army leadership briefings, and inquiries from oversight such as the Government Accountability Office (GAO) and Army Audit Agency (AAA).

h. Ensure the Deputy Assistant Secretary of the Army for Plans, Programs, and Resources verifies that CRM considerations are incorporated into the planning, programming, budgeting, and execution of the Equipping Program Evaluation Group (EE PEG) and Sustaining Program Evaluation Group (SS PEG) functions.

i. Assign the Deputy Assistant Secretary of the Army for Acquisition Policy and Logistics to chair an executive steering group to address unresolved CRM issues.

j. Ensure that CRM is maintained in DA policy and guidance for all appropriate functional areas throughout the equipment and infrastructure life cycles.

1–8. Chief Information Officer

The CIO will—

a. Integrate trusted systems networks (TSN) activities into information assurance controls and other policies and processes, as appropriate, per DoDI 5200.44 and AR 70–77.

b. Issue guidance (for example, information system security engineering guidance) and develop programming recommendations to ensure that TSN concepts and processes are adequately integrated into the acquisition and maintenance of information systems, enclaves, and services, including the purchase and integration of information-communication technology (ICT) commodities.

c. Support the execution of the Army CRM product assurance consistent with applicable roles and responsibilities established in Army regulations and other related policies.

d. Ensure supporting personnel in appointment Information Assurance roles are provided instruction to develop a high level awareness of the CRM process.

e. Appoint a DA Civilian GS–13 equivalent (or above) or military equivalent to act as the primary CRM POC for their organization to the Army counterfeit risk management lead (CRML) within 60 days of promulgation of this regulation. Report the name and contact information to the Army CRML within 15 days of the appointment.

1–9. Deputy Chief of Staff, G–2

The DCS, G–2 will—

a. Provide intelligence, counterintelligence, and threat support to the Army's CRM product assurance based on established policy roles and responsibilities.

b. Support procuring organizations with parts, materials source assessments, and vendor threat assessments to assist with identifying potential risk factors (see DA Pam 702–20).

c. Appoint a DA Civilian GS–13 equivalent (or above) or military equivalent to act as the primary CRM POC for their organization to the Army CRML within 60 days of promulgation of this regulation. Report the name and contact information to the Army CRML within 15 days of the appointment.

1–10. Deputy Chief of Staff, G–3/5/7

The DCS, G–3/5/7 will—

a. Ensure that CRM considerations are incorporated into the planning, programming, budgeting, and execution of Training Program Evaluation Group (TT PEG) functions. Provide a report summarizing CRM requirements in the TT PEG to the Army CRMPL no later than September 30th each year. This report will identify how CRM requirements are articulated in their program budget guidance as well as the funding levels requested, validated, and resourced to execute CRM-related activities over the current year, budget year and Program Objective Memorandum years.

b. Appoint a DA Civilian GS–13 equivalent (or above) or military equivalent to act as the primary CRM POC for their organization to the Army CRML within 60 days of promulgation of this regulation. Report the name and contact information to the Army CRML within 15 days of the appointment.

c. Design and incorporate mandatory CRM training into Soldier and DA programs of instruction as appropriate. At a minimum, focus will cover acquisition, logistics, maintenance, technical, and engineering related career fields.

1–11. Deputy Chief of Staff, G–4

The DCS, G–4 will—

a. Advise the Army CRMPL in the area of CRM and counterfeit threat-related issues pertaining to the functional area of logistics.

b. Support CRM efforts throughout the material's life cycle phases, to include supporting the appropriate Program Evaluation Group (PEG) to plan, program, and budget resources that effectively sustain the CRM product assurance for fielded systems.

c. Evaluate the CRM product assurance's effectiveness by reviewing Army commands (ACOMs), Army service component commands (ASCCs), direct reporting units (DRUs), Army National Guard (ARNG), and U.S. Army Reserve (USAR) CRM survey reports.

d. Ensure that CRM requirements are reflected in DA policies for maintenance, supply, and transportation of equipment for all components of the Army.

e. Provide oversight to ensure implementation of CRM product assurance for Command Maintenance Discipline Programs (CMDPs) are in compliance with the Field Level Requirements Checklist per AR 750–1, DA Pam 750–1, and this regulation for ACOMs, ASCCs, DRUs, ARNG, and USAR CRM product assurance.

f. Appoint a DA Civilian GS–13 equivalent (or above) or military equivalent to act as the primary CRM POC for their organization to the Army CRML within 60 days of promulgation of this regulation. Report the name and contact information to the Army CRML within 15 days of the appointment.

g. Ensure that the primary CRM POC—

(1) Has appropriate background, duties, and responsibilities to carry out this function and the ability to collect and report annually on the required information.

(2) Provides timely, complete, and accurate information in response to all information requests distributed by the Army CRMPL, including but not limited to, annual reporting requirements per paragraph 2–2, status of CRM product assurance for CMDP Field Level Requirements Checklist for commands per AR 750–1 and DA Pam 750–1, internal Army leadership briefings, and inquiries from oversight bodies such as GAO and AAA.

1–12. Deputy Chief of Staff, G–9

The DCS, G–9 will—

a. In coordination with the Assistant Secretary of the Army (Installations, Energy and Environment) (ASA (IE&E)) and the Chief of Engineers (COE), ensure that that CRM is maintained in DA policy and guidance for which DCS, G–9 is the proponent such as, but not limited to, AR 420–1.

b. In coordination with the ASA (IE&E); CG, AMC; and the COE, ensure that policies and procedures are developed and implemented to track and report on counterfeit risks.

c. Appoint a DA Civilian GS–13 equivalent (or above) or military equivalent to act as the primary CRM POC for their organization to the Army CRML within 60 days of promulgation of this regulation. Report the name and contact information to the Army CRML within 15 days of the appointment.

1–13. Chief of Engineers

The COE will—

a. Develop local policies and procedures to establish, manage, and execute a command-level CRM product assurance per paragraph 2–1.

b. In coordination with the ASA (IE&E); DCS, G–9; and CG, AMC, develop implementing guidance for facility planners to create specific measurable, performance-based CRM requirements in the process of tailoring Unified Facilities Guide Specifications, Unified Facilities Criteria, Whole Business Design Guide, or similar documents into a facility design.

c. Follow the additional responsibilities identified in paragraph 1–22.

1–14. Commanding General, U.S. Army Training and Doctrine Command

The CG, USATRADOC will—

a. Develop local policies and procedures to establish, manage, and execute a command-level CRM product assurance per paragraph 2–1 of this regulation.

b. Appoint a DA Civilian GS–13 equivalent (or above) or military equivalent to act as the primary trainer CRM POC for their organization to the Army CRML within 60 days of promulgation of this regulation. Report the name and contact information to the Army CRML within 15 days of the appointment.

c. Ensure that the primary trainer CRM POC includes CRM considerations in all levels of training (basic, follow-on, and advanced individual training) for appropriate military and civilian personnel, including but not limited to logistics, acquisition, storage/maintenance/supply, maintenance support/packaging, and operation specialists. Training will cover sources, identification, detection methods, reporting, and

preventive measures, at a minimum. Ensure course curricula and training materials reflect the current CRM information available from Army CRMPL, AMC, Life Cycle Management Commands (LCMCs) and AFC, Combat Capabilities Development Command (DEVCOM).

d. Oversee the integration of CRM training and education into appropriate curriculum for acquisition, logistics, and maintenance personnel. Training and education should include identifying the causes of counterfeit, detection, and corrective and preventive measures.

e. Develop CRM training curriculums with the Army CRMPL, AMC, and LCMC.

1–15. Commanding General, Army Materiel Command

The CG, AMC will—

a. Serve as the U.S. Army's Primary Office of Responsibility for CRM.

b. In coordination with the ASA (IE&E) and DCS, G–9, ensure that CRM is maintained in DA policy and guidance.

c. In coordination with the ASA (ALT), ensure CRM is addressed in the supportability analysis as it relates to integrated product support in the materials acquisition process.

d. In coordination with the ASA (ALT), ensure CRM is addressed in the LCSPs as it relates to integrated product support in the materials life cycle process.

e. In coordination with DCS, G–4, ensure that CRM considerations are incorporated into the planning, programming, budgeting, and execution of the EE PEG and SS PEG functions.

f. Designate a DA Civilian to serve as the Army CRML who is responsible for coordinating DA-level CRM product assurance activities throughout the Army. The CRML will—

(1) Manage and oversee the central Army CRM office within HQDA.

(2) Ensure that CRM is maintained in DA policy and guidance for all appropriate functional areas throughout the equipment and infrastructure life cycles with ASA (ALT), ASA (IE&E) and DCS, G–9.

(3) Initiate and sustain an effective Army CRM product assurance, evaluate its effectiveness, and ensure the necessary resources are reflected in the planning, programming, budgeting, and execution system.

(4) Serve as the principal POC for the DA to the Deputy Assistant Secretary of Defense for Supply Chain Integration under the Assistant Secretary of Defense for Sustainment within the Office of the Secretary of Defense.

(5) Prepare an annual report evaluating the effectiveness of the Army CRM product assurance and providing recommendations no later than December 31st of each year to ACOMs.

(6) Ensure resources to DEVCOM to support Army CRM product assurance day to day activities.

(7) Provide briefings to MATDEVs upon request for CRM.

(8) Initiate and oversee a CRM working group.

g. Ensure LCMCs conduct command CRM surveys to ensure program compliance and current threat. All survey reports, results, findings, and so forth, are provided to the Army CRML within 90 days of completing the survey.

h. Collect and post CRM survey data and reports from the survey teams to a central repository for Armywide access and to provide the CRM surveys to CRML; ASA (ALT); DCS, G–4; CG, AFC; and the LCMCs. The National Maintenance Manager will ensure that CRM is addressed in the the National Management Program, to include the development of budget requests in support of program requirements.

i. Ensure LCMC assist USATRADOC with the development of CRM training curriculums.

j. Ensure DEVCOM is resourced to provide engineering support and analysis of suspected counterfeit material.

k. Develop and promulgate local policies, processes, and procedures to ensure proactive supply chain risk management and assist the MATDEVs with compliance throughout the life cycle in support of programs of record, sustainment systems, and joint systems that are Army supported.

l. Develop and maintain overarching anti-counterfeit resources and guidance for LCMCs, including the tracking of suspected counterfeit product quality deficiency report (PQDRs) per AR 702–7/DLAR 4155.24/SECNAVINST 4855.21/AFI 21–115/DCMA INST 1102 and AR 702–7–1, and suspected counterfeit Government-Industry Data Exchange Program (GIDEP) data per DoDI 4140.67.

m. Ensure that Army Medical Logistics Command (AMLC) LCMCs—

(1) Appoint a DA Civilian GS–13 equivalent (or above) or military equivalent to act as the primary CRM POC for their organization to the Army CRML within 60 days of promulgation of this regulation. Report the name and contact information to the Army CRML within 15 days of the appointment.

(2) Ensure that the primary CRM POC—

(a) Has appropriate background, duties, and responsibilities to carry out this function and the ability to collect and report annually on the required information.

(b) Provides timely, complete, and accurate information in response to all information requests distributed by the Army CRMPL, including but not limited to, annual reporting requirements, internal Army leadership briefings, and inquiries from oversight bodies such as GAO and AAA.

(3) Consider CRM in the following areas:

(a) Collection, distribution, and feedback of system test and equipment maintenance information.

(b) Army materials acquisition, recapitalization, remanufacture, overhaul, and/or product improvement, including the evaluation of each proposal for a new system, equipment, or component.

(c) Testing and evaluation on the equipment, processes, and application techniques within the assigned areas of responsibility. (This specifically includes nondestructive testing and evaluation of commercial material, equipment, or processes.)

(d) Evaluation of nondevelopmental items, equipment, and systems.

(e) Procurements and supply chain management.

(f) Drafting of medical materials requirements documents.

(g) Direction, evaluation, and coordination of medical materials.

(h) Medical materials maintenance programs.

(i) Medical materials life cycle management.

(j) Procurement, operation, and evaluation of all medical service materials and pharmaceuticals.

(4) Provide information to and support the weapons systems managers.

(5) Develop and provide commodity specific counterfeit risk instructions to address the identification, risk management, consequences, and corrective and preventive measures for appropriate personnel involved in the life cycle sustainment of Army materials.

(6) Ensure that CRM requirements and technologies recommended by the Army CRMPL are incorporated into new designs or in sustainment procedures to achieve acceptable risk thresholds and equipment and pharmaceutical protection.

(7) Annually, or more frequently as required, review CRM processes and procedures of any arsenals and depots under LCMC or AMLC.

(8) Assist the Army CRMPL to ensure adequate CRM planning for MATDEVs SEP/SAMPs and LCSP documents.

n. Ensure the logistics assistance representative—

(1) Has appropriate background, duties, and responsibilities to carry out this function and the ability to collect and report any information on suspected counterfeit materials and parts between their command and the commands they support.

(2) Captures and responds to notifications of suspected and confirmed counterfeit parts and materials from the respective commands they are supporting.

1–16. Commanding General, U.S. Army Futures Command

The CG, AFC will—

a. Develop local policies and procedures to establish, manage, and execute a command-level CRM product assurance per paragraph 2–1.

b. In coordination with the DCS, G–3/5/7, develop implementing guidance to create written, measurable, performance-based CRM requirements in the process of translating capability requirements into system and performance requirements and specifications for use in CRM planning in accordance with DoDI 4140.67. Review the guidance annually and provide copies to the Army CRML within 30 days of initial publication and revision.

c. In coordination with the ASA (ALT), plan, program, budget, and execute an RDT&E program to investigate new materials and technologies for CRM for Army equipment. Ensure that this RDT&E program includes efforts to develop and maintain accelerated counterfeit testing capabilities.

d. In coordination with the DCS, G–4, ensure that CRM considerations are incorporated into the planning, programming, budgeting, and execution of the EE PEG and SS PEG functions.

e. Ensure that CRM is adequately addressed by the cross-functional teams (CFTs) as early as possible in the combat systems development and prototyping processes and that lessons learned are provided to PEOs, PMs, and MATDEVs for refinement of their CRM planning efforts.

f. Ensure that capability developers include CRM considerations in the initial development of documented LCSPs in accordance with AR 700–127 and DA Pam 700–127.

g. Ensure that the CG, DEVCOM; the Director, Futures and Concepts Center; the Directors, CFTs; and the Directors, DEVCOM Centers and Laboratories each appoint a DA Civilian GS–13 equivalent (or above) or military equivalent to act as the primary CRM POC for their organization to the Army CRML within 60 days of promulgation of this regulation or of a vacancy of the position and have reported the names and contact information to the Army CRML within 15 days of the appointment.

h. Assist USATRADOC with the development of CRM training curriculums.

i. Provide engineering support to investigate and analyze suspected counterfeit material.

j. Manage the activities of the Army CRM product assurance.

1–17. Commanding General, U.S. Army Cyber Command

The CG, USARCYBER will—

a. Develop local policies and procedures to establish, manage, and execute a command-level CRM product assurance per paragraph 2–1.

b. Develop CRM processes for the cyber supply chain that encompass both the inbound and outbound supply chains.

c. Enforce Joint Federated Assurance Center's guidance and practices in the areas of:

(1) Software assurance.

(2) Hardware assurance.

(3) Technology transfer.

d. Follow the additional responsibilities identified in paragraph 1–22.

1–18. Commanding General, U.S. Army Test and Evaluation Command

The CG, ATEC will—

a. Provide counterfeit testing and evaluation support that is requested and funded by PMs and other programs throughout the Army.

b. Notify PMs of all occurrences of suspect and confirmed counterfeit materials or parts that are identified during testing and evaluation.

c. Follow the additional responsibilities identified in paragraph 1–22.

1–19. Commanding General, U.S. Army Intelligence and Security Command

The CG, INSCOM will—

a. Develop local policies and procedures to establish, manage, and execute a command-level CRM product assurance per paragraph 2–1.

b. Provide counterfeit risk analysis to CRML, PEOs/PMs, and MATDEVs to mitigate the counterfeit risk to program supply chains.

c. Follow the additional responsibilities identified in paragraph 1–22.

1–20. Director, U.S. Army Criminal Investigation Division

The Director, USACID will—

a. Develop local policies and procedures to establish, manage, and execute a command-level CRM product assurance per paragraph 2–1.

b. Conduct counterfeit investigations to identify and eliminate source of the counterfeit to the U.S. Army supply chain.

c. Follow the additional responsibilities identified in paragraph 1–22.

1–21. Director, U.S. Army Acquisition Support Center

The Director, USAASC will—

a. Develop local policies and procedures to establish, manage, and execute a command-level CRM product assurance per paragraph 2–1.

b. Incorporate CRM processes, procedures, and techniques into all acquisitions, instructions, and sustainment processes as deemed necessary in accordance with DoD and Army regulations and guidance.

c. Follow the additional responsibilities identified in paragraph 1–22.

1–22. Commanders of Army commands, Army service component commands, and direct reporting units

Commanders of ACOMs, ASCCs, and DRUs will—

a. Appoint a DA Civilian GS–13 equivalent (or above) or military equivalent to act as the primary CRM POC for their organization to the Army CRML within 60 days of promulgation of this regulation. Report the name and contact information to the Army CRML within 15 days of the appointment.

b. Ensure that battalion and regiment commanders appoint a respective battalion or regiment CRM POC to act as their respective battalion or regiment CRM POC for their command to the Army CRML and their respective primary CRM POC within 60 days of promulgation of this regulation or of a vacancy of this position. Report the name and contact information to the Army CRML and their commands' primary CRM POC within 15 days of the appointment.

c. Develop local policies and procedures to establish, manage, and execute a command-level CRM product assurance per paragraph 2–1.

d. Host and provide support for CRM Surveys.

e. Ensure that the primary CRM POC—

(1) Has the appropriate background, duties, and responsibilities to carry out this function and the ability to collect and report annually on the required information.

(2) Provides timely, complete, and accurate information in response to all information requests distributed by the CRML, including but not limited to annual reporting requirements per paragraph 2–2, internal Army leadership briefings, and inquiries from oversight bodies such as GAO and AAA.

(3) Provides feedback and guidance to MATDEVs on CRM contract requirements to bolster prevention of counterfeit parts.

(4) Develops and updates a command-level CRM product assurance at least every 3 years.

(5) Maintains CRM in policy and guidance, as applicable to their organization, and identifies the funding levels associated with CRM activities in *paragraph 1–24a*.

f. Confirms that the battalion and regiment CRM POC develops and implements unit CRM product assurance.

1–23. Program executive officers and materiel developers

PEOs and MATDEVs will—

a. Develop local policies and procedures to establish, manage, and execute a command-level CRM product assurance per paragraph 2–1.

b. Develop the technical verification requirements of all items during procurements, with initial focus on electronic parts.

c. Conduct assessments of government contractors and vendors to ensure CRM requirements for monitoring, detecting, and reporting of suspected counterfeit parts are in place and being followed.

d. Appoint a DA Civilian GS–13 equivalent (or above) or military equivalent to act as the primary POC for their organization to ASA (ALT) within 60 days of promulgation of this regulation or of a vacancy of this position. Report the name and contact information to ASA (ALT) within 15 days of the appointment.

1–24. Counterfeit risk management leads

Organization CRMLs will—

a. Ensure that CRM is maintained in policy and guidance for each of the following, as applicable to their organization, and identify the funding levels associated with CRM activities in each area:

(1) System acquisition and production.

(2) Design and maintenance activities.

(3) RDT&E programs and activities.

(4) Equipment standardization programs and including international standardization agreements.

(5) Logistics research and development initiatives.

(6) Logistics support analysis as it relates to integrated logistic support in the materials acquisition process.

(7) Military infrastructure design.

(8) Construction.

(9) Maintenance activities.

b. Provide prompt responses to CRML questions, requests for information and assistance, and annual reporting requirements.

c. As required, develop, implement, and document their respective command CRM product assurance throughout the life cycle, which will include annual reporting requirements. See paragraph 2–2.

d. Participate in CRM surveys as needed, review the resultant findings, lessons learned, reports, data, and so forth, and coordinate follow-on actions with their respective organization.

Chapter 2
Counterfeit Prevention

Section I

General

2–1. Policy

a. Known counterfeit materials or parts will not be procured.

b. A risk-based approach will be documented and employed when procuring materials or parts to reduce the frequency and mitigate the impact of counterfeit components within acquisition and life cycle sustainment processes by—

(1) Applying prevention and early detection procedures to minimize the presence of counterfeit parts and materials within the supply chain as the primary strategy in eliminating counterfeit components.

(2) Requiring strong oversight and surveillance procedures for critical components as identified by AR 70–77 and all electronic parts as required by Public Law 112–81 (PL 112–81) and as defined in DoDD 5000.01, DoDI 5000.02, DoDI 5000.83, AR 700–127, DA Pam 95–9/SECNAVINST 4140.2/AFI 20–106/DLAI 3200.4/DCMA INST CSI (AV), and DoDI 5200.44.

(3) Incorporating CRM requirements into contracts to ensure clear understanding of counterfeit prevention, detection, monitoring, and reporting requirements.

c. All occurrences of suspect and confirmed counterfeit materials or parts will be documented within 60 days in the Product Data Reporting and Evaluation Program (PDREP) and GIDEP.

d. Approved counterfeit notification repository tools will be employed for rapid, frequent, and thorough screening and qualification of vendors, subcontractors, and suppliers throughout the life cycle of the product.

e. Information about counterfeiting will be made available and accessible at all levels of the Army supply chain as a method to prevent further counterfeiting.

f. All cases of suspected counterfeit parts and materials will be investigated, analyzed, and assessed.

g. Restitution will be sought when cases are confirmed and prescribed remedies obtained by relevant authority including DoDI 7050.05 and the FAR Part 46.

h. Army criminal investigative organizations, intelligence authorities, and those who use the suspect or confirmed counterfeit materials or parts will be notified of incidents at the earliest opportunity.

i. Upon completion of the investigation, materials still believed to be counterfeit are to be destroyed or mutilated to ensure they do not re-enter the supply chain, per DoDM 4160.21 Volume 1.

j. Anti-counterfeit processes will be aligned to support the DoD supply chain goals found in DoDI 4140.67 for:

(1) Weapon system availability.

(2) Weapon system support effectiveness and efficiency.

2–2. Annual report

a. The Army CRML develops and disseminates an information request to all Army organizations annually, including additional implementing guidance as necessary.

b. The primary CRM POCs required by this regulation ensure that their organizations provide timely, complete, and accurate responses to the Army CRML.

2–3. Life cycle approach

The following activities will be documented throughout the life cycle:

a. Procurement of critical components as identified by AR 70–77 and all electronic parts as required by PL 112–81 conducted in accordance with DoDD 5000.01, DoDI 5000.02, DoDI 5000.83, AR 700–127, DA Pam 95–9/SECNAVINST 4140.2/AFI 20–106/DLAI 3200.4/DCMA INST CSI (AV), and DoDI 5200.44.

b. Parts and materials that are susceptible to counterfeiting as determined by either the cognizant engineering support activity leader or by the program management officer.

c. Implementation of anti-counterfeiting measures, strategies, plans, and programs that balance the risks caused by materials or parts identified in paragraph 2–5, with the impact to readiness and cost of the measures.

d. The procurement of critical components and all electronic parts from suppliers that meet appropriate counterfeit avoidance criteria and apply additional appropriate CRM measures when such suppliers are not available.

e. Incorporation of Army anti-counterfeiting procedures throughout the Army supply chain in accordance with Federal and DoD statutes and issuances.

f. Implementation of item unique identification using unique item identifier, specifically for critical components and all electronic parts that are susceptible to counterfeiting to enable authoritative life cycle traceability (see AR 700–145).

g. Implementation of policy to detect counterfeit parts and materials using sampling techniques, materials testing, and auditing in accordance with DoDD 5000.01.

h. Implementation of policy to investigate the occurrence of suspect and confirmed counterfeit parts and materials. All results of investigations regarding counterfeit materials or parts will be reported to the appropriate authorities, deficiency reporting systems, PDREP (the official program of record for the suspected counterfeit within the Army), and GIDEP.

i. Develop, establish, and maintain performance metrics to assess the risks posed by counterfeit parts and materials, and monitor the effectiveness and efficiency of anti-counterfeit measures and actions.

j. Remedy the consequences of counterfeit parts and materials in the supply chain following existing processes and procedures for nonconforming parts and materials described in DoDI 4140.01, DoDI 5000.64, DoDD 5000.01, and the Defense Federal Acquisition Regulation Supplement (DFARS).

k. All occurrences of suspect and confirmed counterfeit materials or parts will be reported to:

(1) Army criminal investigative organizations and other Army law enforcement authorities, GIDEP, PDREP, and any additional organization specific deficiency reporting systems as soon as possible; no later than 60 calendar days of discovery.

(2) The product manager, PM, and contracting officer within 5 days of discovery.

(3) Other DoD components to maintain weapons systems operational performance and preserve life or safety of operating personnel immediately.

Note. Expedite notification when critical components or electronic parts are identified as suspect counterfeit.

Section II

Milestone Activities

MATDEVs will apply the activities listed in this section during the identified acquisition phase. Acquisition programs not following the traditional milestone activities are still expected to follow CRM practices as described.

2–4. Pre-Milestone A (material solution analysis phase)

The potential industrial sectors of the technology are to be evaluated to identify current risk trends and potential bad actors related to sources of technology being considered for design into the parts and material solution. An industrial base technology capability assessment is broad in scope to determine areas of risks for potential technology, industrial and parts and material sectors, and associated supply chains. The assessment must incorporate operational security, supply chain risk management, cause and effect of risks, and any critical technology that is incorporated into the program of record. An example of this is an overall system technology counterfeit risk assessment performed on all critical technology and components which have a high probability of being sourced from nations that have displayed counterfeit trends or have been previously identified as sources of counterfeit. DA Pam 702–20 provides some possible questions for the assessment. The assessment will be sent to the appropriate PM for review prior to proceeding into Milestone A. The scope of this assessment will incorporate the following factors:

a. The probability of the proposed technology being counterfeited.

b. Current shortfalls in the trusted industry sectors.

c. Percent of first time sources of supply.

d. Dependence on sources which could experience a shift in social economic posture.
e. Sources in countries which are labeled less than favored nation status.
f. Incorporation of counterfeit prevention language in program of record's LCSP.

2–5. Milestone A to Milestone B (technology maturation and risk reduction phase)
The risks of counterfeiting will be considered during the activities of the preliminary design review before Milestone B. The design will be evaluated to determine the associated risks of all critical components and all electronic parts based on material and function. This roadmap of components is mandatory and will be recorded as part of the Parts Management Plan.

a. Protection planning. In support of AR 70–77, include a description of the plan (or reference the Counterfeit Prevention Plan) to prevent microelectronic counterfeits (of any kind) in critical components when items are not obtained from the original equipment manufacturer (OEM), original component manufacturer (OCM), or from an authorized distributor.

b. Parts and material. When determining the best parts and material to be used, the long-term availability of the parts and material and any intermediate inputs need to be considered. The long-term availability is determined by the stability of the supply chain from internal and external forces. This includes factors such as:

(1) The stability of the region where parts and material is produced, due to more challenging delivery of parts and materials from volatile regions.
(2) Access to intermediate inputs to the process, such as qualified personnel or raw materials.
(3) The financial health of the manufacturer.
(4) The demand for the parts and material or intermediates.
(5) The profitability of the parts and material, especially for parts that contain sole sourced parts and materials.
(6) Contractor reliability as determined in DA Pam 702–20.

c. Part criticality. The function of the part is tied into the criticality.

(1) If a part is more critical, any unexpected failure could have catastrophic consequences to the safety of the Soldier and the success of the mission.
(2) Parts that have a critical role will be carefully examined for any potential sources of counterfeit.
(3) If a high possibility of counterfeit is suspected, the part is to be reviewed for potential redesign opportunities.

d. Risk factors and likelihood. Certain factors increase the likelihood of a part to be counterfeit with obsolescence and parts and material shortages being the most common factors.

(1) If the part is no longer profitable for the manufacturer to produce, they may eliminate the supply chain.
(2) Unauthorized suppliers may enter in the market offering cheaper goods with expedited delivery. Parts sold in large quantities are a common target for unauthorized suppliers with cheap goods.
(3) Components may be recycled, inferior, or misrepresented.
(4) Counterfeit is common in electronic components that can be easily recycled from electronic waste.
(5) Counterfeit is also common in engine accessories, pipe and tubing, and hardware and abrasives.

e. Consequences. The likelihood of counterfeiting occurring is to be considered closely with the impact of the occurrence.

(1) All parts are to be evaluated to determine the likelihood of counterfeit and the potential consequence.
(2) Counterfeit parts are unlikely to be caught during initial material testing and often fail unexpectedly before the predicted time of failure.
(3) Parts that fail before expected can result in the failure of critical mission functions or endanger the health of personnel.

2–6. Milestone B to Milestone C (engineering and manufacturing development phase)
a. MATDEVs will—

(1) Require all applicable contract procurements implement DFARS 246.870. For procurements where DFARS 246.870 does not apply, require all procurements follow paragraph 2–10.
(2) Promote a community of practice within the United States, DoD activities, and Government and non-Government activities for sharing of information in order to identify best practices and methodologies

for improving the management, identification, testing, and mitigation of the associated risks of counterfeit parts and materials.

(3) Establish and manage a web portal for the provisioning policies, processes, instructions, and community of practice, to be employed for rapid, frequent, and thorough screening and qualification of vendors, subcontractors, and suppliers.

(a) Track and assess suspected counterfeit PQDRs per AR 702–7/DLAR 4155.24/SECNAVINST 4855.21/AFI 21–115/DCMA INST 1102 and AR 702–7–1, and suspected counterfeit GIDEP data per DoDI 4140.67.

(b) A quality management system that traces all components that pass through from suppliers and secondary contractors and secondary contractors and suppliers to maintain quality systems and documentation for all parts and a list of approved suppliers will be maintained by the contractors.

(c) A quality management system that accounts for inventory and a set measure of quality for all parts based on an explicit checklist of specifications provided by the acquisition personnel.

(d) Documentation for all processes and parts is critical for both the primary contractors and any secondary contractors. The manufacturer's personnel will be trained to spot counterfeit within the supply chain and have documented procedures for reporting suspected items.

(4) Oversee and implement additional duties as described in DA Pam 702–20.

b. The engineering support activity leaders will—

(1) Evaluate each component and identify electronic parts that require special contracting processes to mitigate counterfeiting.

(2) Evaluate all other parts and ensure the appropriate level of verification is included in the technical data requirements documents for inclusion into the procurement contract.

c. The contracting officer will—

(1) Include the following DFARS clauses in all electronic parts procurements:

(a) DFARS 252.246–7007.

(b) DFARS 252.246–7008.

(c) DFARS 252.244–7001.

(2) Include the necessary contract data requirements list and data item descriptions to support the DFARS counterfeiting clauses.

(3) Include the appropriate contractual language necessary to require the contractor to comply with all technical requirements.

(4) Conduct start of work meetings with each contractor to ensure they understand their responsibilities and requirements as it pertains to counterfeiting.

d. The primary contractor or OEM/OCM directly supplying any parts or materials to the U.S. Government is required to have a demonstrated system of quality that includes a documented plan to reduce the potential for counterfeit entering into their supply chain and flow-down of requirements to secondary contractors per DFARS 246.870.

2–7. Post Milestone C (production, deployment, and sustainment phase)

The following factors will be reviewed and implemented:

a. Obsolescence. A robust Diminishing Manufacturing Sources and Material Shortages (DMSMS) Plan will be developed to help counter the effects of obsolescence on the supply chain. This plan will include where parts are intended to be purchased from as the part becomes obsolete.

b. Authorized suppliers. Parts will be purchased from the OEM/OCM to the greatest extent possible. In cases where this is not possible, parts will be purchased from an authorized supply chain. Authorized aftermarket suppliers have agreements with the OEM/OCM and have the rights from the OEM/OCM to sell the parts. All elements in an authorized supply chain receive parts only from the OEM/OCM or an authorized supplier. This reduces the risk of counterfeit by ensuring authentic parts are used.

c. Unauthorized suppliers. Purchasing through authorized supply chains becomes more difficult as the part becomes obsolete. The OEM/OCM and any authorized suppliers may have left the market, with parts only available through unauthorized suppliers.

(1) Before a part is acquired from the unauthorized supplier, the part is to be evaluated for:

(a) The potential of replacing the obsolete parts and material with new parts and material from an authorized supplier.

(b) Redesigning the part to remove the obsolete parts and material altogether.

(2) If replacing or redesign as stated in paragraph 2–7c(1) is not possible, then the intended unauthorized supplier will be evaluated rigorously for compliance with standards and risk of counterfeit parts and material.

(a) Unauthorized suppliers should be inspected onsite for counterfeit risk mitigation procedures. The unauthorized supplier will have documentation of their approved suppliers and justification concerning why their suppliers are a low risk. All parts from the unauthorized supplier will be inspected upon delivery. After initial visual inspection, parts will be tested and may be sent to an independent testing lab for further investigation. A part that is nonconforming often needs further evaluation before being reported as suspect counterfeit.

(b) The nonconforming or suspect shipment will be removed entirely from the supply chain and placed in a secure area.

(c) Suspect parts will not be sent back to the supplier to avoid the parts re-entering the supply chain or being sold to another customer. Parts deemed as acceptable through testing will re-enter supply chain classified as acceptable for application.

(d) The suspect parts will be communicated immediately to supervisors and recorded in GIDEP and PDREP within 60 days per FAR 46.317 and FAR 52.246–26.

(e) Use the checklist in DA Pam 702–20 for suspect counterfeit parts.

d. Procurement planning for lead time. The procurement planning process will address long lead time items that are common for many part commodities, and especially for many electronic part classes that can approach 52 weeks for COTS parts. Proper planning can assure availability through authorized suppliers.

e. End of service life. Parts and materials that have reached the end of their useful life will be taken to the proper disposal authorities and damaged beyond all function to ensure they are not recycled back into the supply chain. This includes proper disposition of specialized equipment created for the disposed materials or parts.

2–8. Instructions

a. All personnel supporting acquisition programs and other procurement organizations, including life cycle logisticians and maintenance personnel, who work with critical components or electronic parts at high risk for counterfeiting will receive general anti-counterfeiting instruction and training will be obtained in accordance with the resources listed in DA Pam 702–20.

b. Personnel involved in the management of parts (electronics and non-electronics) will receive instruction in anti-counterfeiting techniques that focus on prevention, detection, mitigation, and disposition of counterfeit parts and materials.

c. Instruction records must be kept and reported annually to the Army CRML.

2–9. Contracting

MATDEVs and AMC personnel will ensure—

a. CRM requirements are incorporated into contracts to ensure clear understanding of counterfeit prevention, detection, monitoring, and reporting requirements.

b. DFARS subpart 246.870 is implemented for covered procurements.

c. For procurements where DFARS 246.870 does not apply, the solicitation requires contractors (and their subcontractors at all tiers flow-down requirements) who obtain critical components, electronic parts, or high-risk materials or parts to implement a risk mitigation process as follows:

(1) If the material or part is currently in production or currently available, solicitations will require the item to be obtained only from the original manufacturers or authorized suppliers.

(2) If the item is not in production or currently available from authorized suppliers, solicitations will require the item to be obtained from suppliers that meet appropriate counterfeit avoidance criteria.

(3) Require the contractor to notify the contracting officer when critical components, electronic parts, or high-risk materials or parts cannot be obtained from an authorized supplier.

(4) Require the contractor to take mitigating actions to authenticate the materials or parts if purchased from an unauthorized supplier.

(5) Require the contractor to report instances of counterfeit and suspect counterfeit parts and materials to the contracting officer and the GIDEP as soon as the contractor becomes aware of the issue.

2–10. Statement of work

MATDEVs and AMC personnel will ensure that the statement of work (SOW) includes additional counterfeit safeguards language, including DFARS 252.246–7007 and DFARS 252.246–7008, as applicable, tailored to the risk and type of material or part. The SOW will include the CRM plan requirements in proper contractual language to reduce ambiguity with potential contractors.

Chapter 3
Risk Management

Section I

General

3–1. Materiel developer counterfeit risk management assessment

a. To properly assess counterfeit risks and ensure sourcing decisions are based upon current and relevant data, MATDEVs, in concert with the OEM, will employ approved resources and processes to enable rapid, frequent, and thorough screening and qualification of vendors, subcontractors, and suppliers.

b. MATDEVs will conduct a CRM assessment and determine the risk of counterfeit. (See DA Pam 702–20.)

c. The assessment will be completed prior to the preliminary design review and reviewed during all following applicable systems engineering technical reviews and during the engineering change proposal process.

d. The assessment will include:

(1) Technology roadmap of the parts and materials selected and the long-term availability of the parts and materials.

(2) Stability of the suppliers and location (region) of the suppliers.

(3) Critical functionalities identified as part of the Program Protection mission.

(4) Criticality of the item and components.

(5) Critical application items.

(6) Susceptibility to counterfeiting certifications used for type classification (TC) are authorized for use in satisfying materiel release (MR) requirements when stated for dual use by the functional authority unless changes were made to the item. The TC and MR processes ensure standard/full materials release at full-rate production to verify the item is safe, suitable, and logistically supportable.

(7) Alignment of Risk Management Framework per DoDI 8510.01, which includes the appropriate methods, standards, and practices required to protect DoD information technology.

3–2. Risk management documents

MATDEVs will—

a. Document critical components, electronic parts, items at high risk of counterfeiting, and counterfeit mitigation processes within the appropriate program plans.

b. Integrate counterfeit detection and avoidance processes into the appropriate program planning processes to the degree identified in the PPP. The program documents include:

(1) *Risk management plan.* The risk management plan will include the specific requirements and criteria to assess the risk of parts and materials to counterfeiting, which is based on criticality of the item and criticality in its application. It will identify anti-counterfeit risk mitigation actions for materials or parts identified as critical components, electronic parts, or having a high risk of being counterfeited.

(2) *System engineering plan.* The SEP will reflect how parts and materials assessed to be at risk for counterfeiting are managed during design and production, such as a robust parts and materials management plan.

(3) *Program protection plan.* The PPP will outline supply chain management risks related to TSN and protecting ICT (see DoDI 5200.44 and AR 70–77).

(4) *Life cycle sustainment plan.* The LCSP will include information on the process for selecting, procuring, and testing materials or parts identified as high or moderate counterfeit risk during sustainment. It may point to other documents as necessary, such as the PPP, if applicable.

(5) *Diminishing manufacturing sources and material shortages management plan.* DMSMS management plan will include:

(a) Actions taken to identify and minimize the DMSMS impact on logistics support efforts.
(b) Procedures to resolve problems created by DMSMS and reduce or eliminate any negative impacts.
(c) Actions to review DMSMS throughout the life cycle by anticipating potential DMSMS occurrences and taking appropriate logistics, acquisition, and budgeting steps to prevent DMSMS from adversely affecting readiness or total ownership cost.
(d) Response actions to DMSMS issues, particularly when those items threaten to degrade weapon system readiness below established goals.
(e) Established DMSMS activities to reduce or eliminate the cost and schedule impacts of all identified DMSMS problems and help ensure that DMSMS problems do not prevent weapon system readiness and performance goals from being met.

Note. Factor in the additional costs of authentication and risk of installing counterfeit parts for any DMSMS resolution that includes purchasing material from unauthorized suppliers.

(6) *Prohibited parts materials and processes.* The prohibited parts materials and processes plan documents the processes used to minimize the risk of procuring and/or using counterfeit parts and materials. The plan will address counterfeit parts and materials prevention and detection methodologies. These methodologies will include at a minimum:
(a) Maximizing availability of authentic, originally designed and/or qualified parts throughout the product's life cycle, including management of parts obsolescence.
(b) Assessing potential sources of supply to minimize the risk of receiving counterfeit parts or materials.
(c) Maintaining a listing of approved suppliers with documented criteria for approval and removal of suppliers from the list.
(d) Certificate of compliance and supply chain traceability for all electronic part purchases.
(e) Minimum inspection and test methods to detect potential counterfeit parts and materials found within the technical requirements.
(f) Instruction of personnel in counterfeit avoidance and detection practices.
(g) Flow-down of counterfeit parts and materials prevention and detection requirements to subcontractors.
(h) Reporting counterfeit parts and materials to other potential users and Government investigative authorities.

Section II

Supplier

3–3. Selection and procurement
To minimize counterfeit risk, parts and materials will only be purchased from the OEM/OCM or an authorized supplier when available. If an unauthorized supplier is the only available source, the supplier will be assessed before being considered a low risk supplier. Vendor screening and qualification is key to counterfeit prevention. There is a vast array of resources available for vendor screening and qualification. Acquisition procedures will allow the technical authority for each purchase to determine supplier suitability based on the supplier confidence assessment results (see DA Pam 702–20).

3–4. Detection and inspection requirements
a. Parts purchased from an unauthorized supplier, critical components, and electronic parts will be inspected and/or tested to establish an acceptable level of confidence in item authenticity.
b. All critical safety items will be thoroughly inspected/tested, regardless of source of supply.
c. The acquisition manager and the supporting engineer will determine the item criticality and the acceptable level of risk and decide on the level of inspection and/or testing rigor required.
d. The failure analysis process will include the analysis for counterfeit parts and materials, especially for recurring trends or unexpected low reliability.

3–5. Detection protocols
a. In the event a low risk supplier cannot be used, mitigating actions to authenticate the item through inspection and/or testing will be taken to determine whether the item is likely counterfeit. Basic counterfeit

detection techniques, such as verifying consistency within paperwork and visually inspecting items and its packaging, will be integrated into the receiving process for all items regardless of the supplier.

b. For parts and materials that are considered high risk, the engineering support activity will develop the counterfeit detection techniques tailored to the item type. Evaluation will be performed before the item is deemed acceptable for introduction into the supply chain.

Chapter 4
Reporting

4–1. Reporting requirements

a. Each occurrence of suspect counterfeit must be reported to the appropriate law enforcement agency, the contracting officer, the pertinent chain of command, and all users of the item.

b. Counterfeit and suspect counterfeit items will be reported through the Army's PQDR system available at https://pdrep.csd.disa.mil/pdrep/pdrephome.action.

c. Reports will be filed with GIDEP within 60 days, unless instructed otherwise by investigating authorities.

d. The GIDEP will be reviewed periodically by procuring organization to assess new GIDEP reports for counterfeit parts and materials. The review will include evaluating reported counterfeit part numbers used in the contractors or subcontractor systems, as well as whether the reported supplier has provided prior materials or parts to the contractor that may not have been authenticated per industry or DoD adopted standards. The GIDEP Operations Manual is available at https://www.gidep.org/about/opmanual/opmanual.htm.

4–2. Containment

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

(1) Notify the program office, contracting officer, and USACID immediately when suspect counterfeit items are identified.

(2) Secure the parts and materials and mark external packaging to denote it is suspect counterfeit to prevent it from re-entering the supply chain.

(3) Under no circumstances will suspect counterfeit materials or parts be returned to the supplier, even if this refusal results in lost reimbursement costs. Do not contact the supplier about the suspect counterfeit items. Requests for analysis will be referred to the OEM/OCM, unless the OEM/OCM is suspected of involvement.

(4) As part of the containment process, personnel will determine the possibility of additional counterfeit materials or parts by investigating prior purchases of—

(a) Any items from that supplier; or

(b) Purchases of the same lot and date code from other suppliers.

b. All potential hardware items with the suspect items will be identified and the users notified.

4–3. Disposition

a. Counterfeit parts and materials represent a performance risk that is impossible to quantify, since the items may have been exposed to unquantified stresses (mechanical, thermal, electrical, chemical, and so forth) or be functionally inferior to its advertised capabilities (designed and tested to a lesser specification). For this reason, suspect counterfeit parts and materials will be removed and replaced.

b. Suspect or confirmed counterfeit parts and materials will not be scrapped or otherwise disposed of without approval from investigative authorities and legal (if involved) or the contracting officer.

c. Parts and materials will be provided upon request to investigative agencies for ongoing investigation or prosecution.

d. Parts and materials deemed unacceptable must be destroyed upon authorization to prevent reintroduction into the supply chain.

e. Methods to destroy parts and materials may include, but are not limited to, shredding or crushing of small electronics and parts and drilling of pressure containing parts to purposely breach the pressure boundary.

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 are available at https://www.acquisition.gov/dfars. DoD publications are available on the Executive Services Directorate website at https://www.esd.whs.mil/dd/.

AR 70–1
Army Acquisition Policy (Cited in *para 1–7e.*)

AR 70–77
Program Protection (Cited in *para 1–7d*.)

AR 420–1
Army Facilities Management (Cited in *para 1–12a*.)

AR 700–127
Integrated Product Support (Cited in *para 1–7e.*)

AR 700–145
Item Unique Identification (Cited in *para 2–3f.*)

AR 702–7/DLAR 4155.24/SECNAVINST 4855.21/AFI 21–115/DCMA INST 1102
Product Quality Deficiency Report Program (Cited in *para 1–15l.*)

AR 702–7–1
Reporting of Product Quality Deficiencies within the U.S. Army (Cited in *para 1–15l.*)

AR 750–1
Army Materiel Maintenance Policy (Cited in *para 1–11e*.)

DA Pam 95–9/SECNAVINST 4140.2/AFI 20–106/DLAI 3200.4/DCMA INST CSI (AV)
Management of Aviation Critical Safety Items (Cited in para 2–1b(2).)

DA Pam 700–127
Integrated Product Support Procedures (Cited in *para 1–7e.*)

DA Pam 702–20
Counterfeit Risk Management Product Assurance Handbook (Cited in para 1–1.)

DA Pam 750–1
Commanders' Maintenance Handbook (Cited in *para 1–11e*.)

DFARS 246.870
Contractors Counterfeit Electronic Part Detection and Avoidance (Cited in para 2–6a(1).)

DFARS 252.244–7001
Contractor Purchasing System Administration (Cited in para 2–6c(1)(c).)

DFARS 252.246–7007
Contractor Counterfeit Electronic Part Detection and Avoidance System (Cited in para 2–6c(1)(a).)

DFARS 252.246–7008
Sources of Electronic Parts (Cited in para 2–6c(1)(b).)

DoDD 5000.01
The Defense Acquisition System (Cited in para 2–1b(2).)

DoDI 4140.01
DoD Supply Chain Materiel Management Policy (Cited in *para 2–3j.*)

DoDI 4140.67
DoD Counterfeit Prevention Policy (Cited on title page.)

DoDI 5000.02
Operation of the Adaptive Acquisition Framework (Cited in *para 1–7e.*)

DoDI 5000.64
Accountability and Management of DoD Equipment and Other Accountable Property (Cited in *para 2–3j*.)

DoDI 5000.83
Technology and Program Protection to Maintain Technological Advantage (Cited in *para 1–7d.*)

DoDI 5200.44
Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN) (Cited in *para 1–8a*.)

DoDI 7050.05
Coordination of Remedies for Fraud and Corruption Related to Procurement Activities (Cited in *para 2–1g.*)

DoDI 8510.01
Risk Management Framework for DoD Systems (Cited in para 3–1d(7).)

DoDM 4160.21 Volume 1
Defense Materiel Disposition: Disposal Guidance and Procedures (Cited in *para 2–1i.*)

FAR Part 46
Quality Assurance (Available at https://www.acquisition.gov/browse/index/far.) (Cited in *para 2–1g*.)

FAR 52.246–26
Reporting Nonconforming Items (Available at https://www.acquisition.gov/browse/index/far.) (Cited in para 2–7c(2)(d).)

GIDEP Operations Manual
(Available at https://www.gidep.org/about/opmanual/opmanual.htm.) (Cited in *para 4–1d*.)

PL 112–81
National Defense Authorization Act for Fiscal Year 2012 (Available at https://www.congress.gov/public-laws/112th-congress.) (Cited in para 2–1b(2).)

Section II

Prescribed Forms

This section contains no entries.

Appendix B

Internal Control Evaluation

B–1. Function
The function covered by this evaluation is CRM.

B–2. Purpose
The purpose of this evaluation is to assist in evaluating key internal anti-counterfeit controls. It is not intended to cover all controls.

B–3. Instructions
Answers must be based on the actual testing of controls (for example, document analysis, direct observation, interviewing, sampling, simulation, evaluation, and reports). Answers that indicate deficiencies must be explained, and corrective action indicated in supporting documentation. These management controls must be evaluated at least once every year. Certification that the evaluation has been conducted must be accomplished in accordance with AR 11–2 on DA Form 11–2 (Internal Control Evaluation Certification).

B–4. Test questions
a. Has a DA Civilian been identified and assigned to serve as the Army CRMPL who is responsible for overseeing DA-level CRM product assurance activities throughout the Army?

b. Has a DA Civilian been identified and assigned to serve as the Army CRML who is responsible for coordinating DA-level CRM product assurance activities throughout the Army?

c. Have primary CRM POCs with appropriate background, duties, and responsibilities been assigned and trained?

d. Have resources been planned, programmed, and budgeted to develop and maintain adequate command CRM product assurance?

e. Have local policies and procedures to establish, manage, and execute a command-level CRM product assurance been developed?

f. Has the developed command-level CRM product assurance been updated at least every 3 years?

B–5. Supersession
Not applicable.

B–6. Comments
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@army.mil.

Glossary of Terms

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).

Commercial off-the-shelf item
A product, material, component, subsystem, or system sold or traded to the general public in the course of normal business operations at prices based on established catalog or market prices (see MIL–STD–130N).

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 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.

Information-communication technology
See DoDI 5200.44.

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

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.

Materiel developer
See AR 750–1.

Nonconforming part
A product or the component of a product that has not been manufactured, assembled, tested, or inspected in accordance with the terms of a contract, its specifications, or drawings, including military specifications.

Original component manufacturer
See DFARS 252.246–7008(a).

Original equipment manufacturer
See DFARS 252.246–7008(a).

Original manufacturer
See DFARS 252.246–7008(a).

Part
See AR 750–1.

Product quality deficiency
A defect or nonconforming condition detected on new or newly reworked government-owned products, premature equipment failures, and products in use that do not fulfill their expected purpose, operation, or service due to deficiencies in design, specification, materiel, manufacturing, and workmanship.

Product quality deficiency report
See AR 702–7–1. The format used to record and transmit product quality deficiency data.

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.

Remedies
Criminal, civil, contractual, and administrative actions that will be initiated by a commander or official having responsibility over a matter central to a significant procurement fraud case in order to protect DoD interests and to deter future incidents of fraudulent conduct.

Restitution
See DoDI 4140.67.

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
A part in which there is an indication that it may have been misrepresented by the supplier or manufacturer and may meet the definition of fraudulent part or counterfeit part.

Suspect counterfeit
See DoDI 4140.67.

Suspect counterfeit electronic part
See DFARS 252.246–7007(a).

Suspect item
An item in which visual inspection, testing, or other means indicate that it may not conform to established Government or industry-accepted specifications or national consensus standards, or one whose documentation, appearance, performance, material, or other characteristics may have been misrepresented by the supplier or manufacturer.

Traceability
See DoDI 4140.67.

Trusted systems networks
The integration of systems engineering, supply chain risk management, security, counterintelligence, intelligence, information assurance, hardware and software assurance, and information systems security engineering disciplines into a single overarching strategy.

Unique item identifier
See DoDI 4140.67.

SUMMARY

AR 702–20
Counterfeit Risk Management Product Assurance

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

- Prescribes policy for the mandatory procedures assigned in DA Pam 702–20 (throughout).
- Establishes Army policy to identify and report counterfeit material (throughout).
- Assigns responsibilities to principal officials, commanders, and leaders with roles in the prevention of counterfeit activities (chap 1).