DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 4855.20
ASN (RD&A)
22 APR 2015

SECNAV INSTRUCTION 4855.20

From: Secretary of the Navy

Subj: COUNTERFEIT MATERIEL PREVENTION

Ref: See enclosure (1).

Encl: (1) References
(2) Responsibilities
(3) List of Industry Standards
(4) Glossary of Terms

1. Purpose. To establish Department of the Navy (DON) policy to prevent the introduction of counterfeit materiel into DON systems. This instruction implements the requirements of references (a) through (i).

2. Background. Counterfeit materiel is a serious threat to the safety and operational effectiveness of Department of Defense (DoD) systems. Counterfeit materiel affects all supply classes and the impact can be significant. Reference (a) requires DoD Components to integrate and implement anti-counterfeiting policies and practices into all relevant issuances, regulations, guidance, contract requirements, and procedures. It also requires employment of a risk-based approach to reduce the frequency and impact of counterfeit materiel within DoD acquisition systems and life cycle sustainment programs and processes.

3. Applicability. This instruction applies to all DON organizations. It applies to all phases of life cycle management, from identifying an operational requirement, introducing an item into the supply chain, system operations and maintenance, through phase out and retirement.

4. Policy. DON activities shall:

a. Implement a risk-based approach to identify and prevent the introduction of materiel that is at high risk of counterfeiting. This approach shall reduce the frequency and impact of counterfeit materiel in DON systems and the supply

chain. Per references (a) through (i), the DON shall apply preventative measures, early detection processes, strengthened surveillance procedures, and accountable oversight commensurate with the end use application of the materiel in the system or its criticality.

b. Ensure all instances of counterfeit materiel or suspect counterfeit materiel are reported as required by this instruction and references (a) through (i).

5. Responsibilities. Responsibilities for identifying and preventing counterfeit materiel in DON systems change as systems move from acquisition to sustainment. For specific responsibilities, see enclosure (2).

6. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV Manual 5210.1 of January 2012.

7. Forms. SF Form 368, Product Quality Deficiency Report (PQDR) (Rev. 5-2011)is available electronically from the GSA Forms Library at: http://www.gsa.gov/portal/forms/type/TOP.

RAY MABUS

Distribution:
Electronic only, via Department of Navy Issuances Web site:
http://doni.documentservices.dla.mil

REFERENCES

(a) DoDI 4140.67, DoD Counterfeit Prevention Policy of 26 April 2013
(b) Defense Federal Acquisition Regulation Supplement, current edition
(c) DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks of 5 November 2012
(d) Program Protection Plan Outline and Guidance, Deputy Assistant Secretary of Defense for Systems Engineering of 18 July 2011
(e) SECNAVINST 4855.3C, Product Data Reporting and Evaluation Program of 27 June 2014
(f) SECNAVINST 5400.15C CH-1, Department of the Navy Research and Development, Acquisition, Associated Life-Cycle Management, and Logistics Responsibilities and Accountability of 2 December 2011
(g) DoDM 4140.01, DoD Supply Chain Materiel Management Procedures, Volumes 1-11 of 10 February 2014
(h) SECNAVINST 5000.2E, Department of the Navy Implementation and Operation of the Defense Acquisition System and the Joint Capabilities Integration and Development System of 1 September 2011
(i) SECNAVINST 4140.2, Management of Aviation Critical Safety Items of 25 January 2006

RESPONSIBILITIES

1. Deputy Assistant Secretary of the Navy (Expeditionary Programs and Logistics Management) shall:

a. Provide guidance and policy for counterfeit materiel identification and prevention within the DON.

b. Track and assess Product Quality Deficiency Report (PQDR) metrics for the DON to support internal and external reviews for potential counterfeit risk. Negative trends and potential risks identified through assessment of counterfeit metrics will be used to determine if additional anti-counterfeiting measures are needed.

c. Review Life Cycle Sustainment Plans (LCSP) per reference (h) to ensure processes and measures are in place to protect systems from counterfeit materiel during operations and sustainment.

2. Chief of Naval Operations and Commandant of the Marine Corps shall:

a. Provide amplifying, Service-specific guidance and policy for counterfeit materiel prevention as necessary.

b. Direct the actions necessary to ensure counterfeit materiel prevention efforts are incorporated in all aspects of in-service support as defined in reference (f).

3. Systems Commands, Program Executive Offices, Direct Reporting Program Managers, and procuring activities shall:

a. Ensure personnel who are involved with the purchase, inspection, installation, repair, maintenance, and overhaul for new construction and life cycle maintenance of critical materiel or materiel at high risk for counterfeiting receive training commensurate with their duties to prevent, detect, and report counterfeits identified in their systems.

b. As part of the overall technical risk management process:

(1) Assess the design prior to the Preliminary Design Review to determine the risk of counterfeiting to the selected materiel. Consider criticality of the materiel, its application, and susceptibility to counterfeiting in this assessment.

(2) Assess the risk of counterfeits to the system and supply chain throughout the product's life cycle, and review processes to mitigate counterfeit risks as part of the systems engineering technical reviews and in-service reviews.

(3) Conduct assessments to determine the risk of counterfeiting as part of the engineering change proposal process.

(4) Consider all items meeting the definition of "critical materiel" as defined in enclosure (4), as high risk for counterfeiting.

c. Document critical materiel and materiel identified as high risk for counterfeiting in the appropriate program plans.

d. Identify and document anti-counterfeit risk mitigation actions for materiel identified as critical or having a high risk of being counterfeited in the Risk Management Plan or the Systems Engineering Plan.

e. Document specific supply chain management risks associated with Program Protection in the Program Protection Plan, per reference (d). Supply chain management risks related to Program Protection are defined in reference (c).

f. Document processes and measures to protect systems from counterfeit materiel during operations and sustainment in the LCSP. These processes and measures will be periodically assessed during Independent Logistics Assessments.

g. Ensure subpart 246.870 of reference (b) is enacted for all applicable procurements. For procurements where subpart 246.870 of reference (b) does not apply:

(1) Ensure that solicitations require contractors (and their subcontractors at all tiers) who obtain critical or high

risk materiel to implement a risk mitigation process per paragraphs 3g(1)(a) and 3g(1)(b) below.

(a) If the materiel is currently in production or currently available, solicitations shall require the materiel to be obtained only from authorized sources. Authorized sources are the original manufacturer, a source with the express written authority of the original manufacturer or current design activity, or an authorized aftermarket manufacturer.

(b) If the materiel is not in production or currently available from authorized sources, solicitations shall require the materiel to be obtained from suppliers that meet appropriate counterfeit avoidance criteria. Counterfeit avoidance criteria can be found in the Industry Standards identified in enclosure (3).

(2) Require the contractor to notify the contracting officer when critical or high risk materiel cannot be obtained from an authorized source.

(3) Require the contractor to take mitigating actions to authenticate the materiel if purchased from another source.

(4) Require the contractor to report instances of counterfeit and suspect counterfeit materiel to the Contracting Officer and the Government-Industry Data Exchange Program (GIDEP) as soon as the contractor becomes aware of the issue.

(5) Ensure the program office reports instances of counterfeit and suspect counterfeit materiel on a PQDR using the defect attribute code, "5AS Suspect Counterfeit Materiel."

h. Ensure solicitations utilized to support depot maintenance efforts include requirements to identify critical materiel and materiel assessed as high risk for counterfeiting.

i. Ensure all instances of counterfeit and suspect counterfeit materiel that are owned or operated by the government identified in the field, fleet, or depots are reported to the Naval Criminal Investigative Service, the Navy Assistant General Counsel's Acquisition Integrity Office, PQDR reporting systems, and GIDEP per reference (a).

(1) Government and government contract personnel that identify instances of counterfeit and suspect counterfeit materiel shall ensure initiation of a PQDR per reference (e), using the defect attribute code, "5AS Suspect Counterfeit Materiel."

(2) Counterfeit materiel identified at a contractor facility shall be reported to the cognizant program office via the contracting officer and to GIDEP as soon as the contractor becomes aware of the issue.

LIST OF INDUSTRY STANDARDS

The following Industry Standards provide counterfeit avoidance and risk mitigation information. It is not an inclusive list.

1. SAE AS5553A, "Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition" of January 2013. Adopted by DoD.

2. SAE AS6462, "AS5553, Counterfeit Electronic Parts; Avoidance, Detection, Mitigation, and Disposition Verification Criteria" of November 2012.

3. SAE AS6081, "Fraudulent/Counterfeit Electronic Parts: Detection, Mitigation, and Disposition – Distributors" of November 2012. Adopted by DoD.

4. SAE ARP6178, "Fraudulent/Counterfeit Electronic Parts; Tool for Risk Assessment of Distributors" of December 2011.

5. SAE AS6174A, "Counterfeit Materiel; Assuring Acquisition of Authentic and Conforming Materiel" of July 2014. Adopted by DoD.

6. SAE AS6301, "Compliance Verification Criterion Standard for SAE AS6081, Fraudulent/Counterfeit Electronic Parts: Avoidance, Detection, Mitigation, and Disposition – Distributors" of January 2014.

GLOSSARY OF TERMS

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

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

3. Counterfeit Materiel. Items that are unauthorized copies or substitutes that have been identified, marked, or altered by a source other than the items' legally authorized source or have been misrepresented to be authorized items of the legally authorized source.

4. Critical Materiel. Critical Materiel includes:

a. Critical Components as defined in reference (c).

b. Controlled Inventory Items as defined in volume 11 of reference (g).

c. Critical Safety Items as defined in subpart 209.270 of reference (b), volume 11 of reference (g), and references (h) and (i).

d. Critical Application Items as defined in references (g) and (i).

e. Other materiel identified by the responsible engineering support activity prior to initial supportability analysis and documented by the responsible logistics organization. Initial supportability analysis occurs either during the initial provisioning and cataloging process or upon approval of a design change notice.

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

5. Electronic Part. Defined in Section 818, paragraph (f)(2) of PL 112-81-Dec 31, 2011 as "an integrated circuit, a discrete electronic component (including, but not limited to, a transistor, capacitor, resistor, or diode), or a circuit assembly." It also includes any embedded software or firmware.

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

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

8. High Risk. Materiel that has previously been counterfeited or is susceptible to counterfeiting and has an end use or application where the success or security of the mission, or safety of the warfighter, depends on the continued reliable function of the materiel.

9. Materiel. As defined in volume 1 of reference (g), includes material, system components, sub-components, software, and information and communications technology as defined in reference (c). Materiel includes support equipment and systems purchased, procured, contracted, or incorporated into the DoD supply chain for weapon and information systems, DoD business processes, and DoD operational support.

10. Original Manufacturer. An organization that designs and/or engineers a part or materiel and is pursuing or has obtained the intellectual property rights to that part.

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

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