

<p>SUBJECT</p> <p>COUNTERFEIT AVOIDANCE PROCEDURE</p>	<p>Procedure No. 1.0</p> <p>Revision</p> <p>Effective Date: March 27, 2017</p> <p>Supersedes Rev:</p> <p>Date: March 27, 2017</p> <p>Page: 1 of 12</p>
---	--

The National Defense Authorization Act imposes new requirements on defense contractors regarding counterfeit electronic part avoidance. Contractors who fail to comply with these new requirements risk suspension, debarment, and potential civil and criminal liability. This policy covers a) Electrical Parts, and b) Non Electrical Parts (Airworthiness Products).

a) Electrical Parts

All electrical, electronic and electro-mechanical parts delivered and/or used in the manufacture of deliverable products shall be from the Original Component Manufacturer (OCM)/Original Equipment Manufacturer (OEM) or their franchised distributor. Parts shall not be used or reclaimed and misrepresented as new. Parts shall not be acquired from independent distributors or brokers. The supplier must have a certification from the OCM/ OEM, and that certification shall be delivered with each lot/ shipment. Companies that procure electrical, electronic and electro-mechanical parts need to have a Counterfeit Avoidance Policy and Program to ensure it does not receive counterfeit parts into inventory, use them in manufacturing, or inadvertently sell them to other parties.

The supplier shall have a counterfeit avoidance process that meets the intent of SAE standard AS5553, Counterfeit Electronic Parts, Avoidance, Detection, Mitigation, and Disposition. Suppliers that deliver next higher assemblies shall flow this requirement down to all their sub-tier suppliers to prevent the inadvertent use of counterfeit materials and equipment. Suppliers of next higher assemblies shall specify on their purchase order to their sub-tier suppliers that they shall only procure electrical, electronic and electro-mechanical parts from the original manufacturer of the part or the original manufacturer's franchised distributor only.

b) Non-Electrical Parts

Companies that procure non-electrical standard parts need to have a Counterfeit Avoidance Policy and Program to ensure it does not receive counterfeit parts into inventory, use them in manufacturing, or inadvertently sell them to other parties. The supplier shall have a counterfeit avoidance process that is similar to, and meets the intent of, SAE standard AS61743, Counterfeit Non-Electronic Parts, Avoidance, Detection, Mitigation, and Disposition. Suppliers of next higher assemblies shall flow this requirement down to all their sub-tier suppliers to prevent the inadvertent use of counterfeit materials and equipment. Distributors or brokers that supply non-electrical standard parts, like fasteners, nuts, washers, springs, o-rings, inserts, and pins, must have a certification from the Original Component Manufacturer (OCM)/Original Equipment Manufacturer (OEM), and that certification shall be delivered with each lot/ shipment. Parts shall not be used or reclaimed and misrepresented as new.

<p>SUBJECT</p> <p>COUNTERFEIT AVOIDANCE PROCEDURE</p>	<p>Procedure No. 1.0</p> <p>Revision</p> <p>Effective Date: March 27, 2017</p> <p>Supersedes Rev:</p> <p>Date: March 27, 2017</p> <p>Page: 2 of 12</p>
---	--

1.0 PURPOSE

This Policy, and the procedures described within, is intended to detect, avoid, and help abolish the use and proliferation of counterfeit and suspect counterfeit electronic parts at **East Coast Datacom, Inc.**, hereafter referred to as **ECDATA.COM**. With that end in mind, this Policy specifies certain requirements that must be met with respect to procurement and to the identification, control, and disposition of such parts.

2.0 SCOPE

The counterfeit risk mitigation requirements of ECDATA.COM for electronic and non-electronic parts procured from dealers, distributors and brokers are contained in this procedure. For the purposes of this document, ‘electronic’ represents Electrical, Electronic, and Electromechanical (EEE) components hereinafter referred to as electronic parts.

This document provides requirements, practices and methods to mitigate the risks of receiving counterfeit electronic parts. It also specifies requirements for suppliers’ counterfeit risk mitigation and control plan, and applies to all levels of procurement of electronic parts and associated material management, and inspection and test.

A distributor who complies with all the requirements of this document is considered a Counterfeit Electronic Parts Avoidance approved supplier. Allowance to depart from the requirements within this document is at the sole discretion of ECDATA.COM.

3.0 DEFINITIONS

3.1 Authorized/Franchised Distributor

A distributor that has a contractual agreement with the original component manufacturer (OCM) or original equipment manufacturer (OEM) to directly buy, stock, repackage, sell and distribute their product. Authorized/franchised distributors typically provide full manufacturer warranty for the product for sale.

3.2 Approved Trusted Supplier

A non-franchised distributor that has been either: (1) identified as a trusted supplier by the Department of defense pursuant to Section 818 of the 2012 National Defense Authorization Act (Pub. L. No. 11281§818), or (2) audited and preapproved by ECDATA.COM for the purchase of electronic parts unavailable from an OEM or OCM or their authorized dealers.

<p>SUBJECT</p> <p>COUNTERFEIT AVOIDANCE PROCEDURE</p>	<p>Procedure No. 1.0</p> <p>Revision</p> <p>Effective Date: March 27, 2017</p> <p>Supersedes Rev:</p> <p>Date: March 27, 2017</p> <p>Page: 3 of 12</p>
---	---

3.3 Broker/Non-Franchised Distributor

Distributor, not authorized by the OEM/OCM, who may not carry inventory but will search industry to locate parts that meet the target price and other customer requirements. Brokers may also purchase excess inventories from end users or other sources with the intention to sell and redistribute.

3.4 Counterfeit Electronic Part

A part made or altered to imitate or resemble an approved part without authority or right, and with the intent to knowingly mislead or defraud by passing the imitation as original or genuine. A part whose identity has been deliberately altered, misrepresented, or falsified. This definition includes used parts represented as new.

Electronic Part – As used in this document, the term “electronic part” refers to any integrated circuit, discrete electronic component (including, but not limited to, a transistor, capacitor, resistor or diode), or circuit assembly.

3.5 Original Component Manufacturer (OCM)/ Original Equipment Manufacturer (OEM)

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

3.6 Seller

For the purpose of this specification; A seller is an entity that meets the requirements of this specification and provides electronic parts that are in accordance with a contract or purchase order.

3.7 Suspect Electronic Parts

A suspect electronic part is an indication established by inspection, testing, or other means that its authenticity may have been misrepresented by the supplier and may be counterfeit. A copy or substitute created without benefit of legal right or authority to do so or one whose material, performance, or characteristics have been knowingly misrepresented by a supplier in the supply chain is also a suspect electronic part.

<p>SUBJECT</p> <p>COUNTERFEIT AVOIDANCE PROCEDURE</p>	<p>Procedure No. 1.0</p> <p>Revision</p> <p>Effective Date: March 27, 2017</p> <p>Supersedes Rev:</p> <p>Date: March 27, 2017</p> <p>Page: 4 of 12</p>
---	--

Examples of counterfeit electronic parts include, but are not limited to:

- a. Electronic parts that do not exhibit the proper internal construction consistent with that ordered e.g., incorrect die, multiple die sizes with one date code, wrong manufacturer, wire bonding, etc.;
- b. Used, refurbished or reclaimed electronic parts represented as new product;
- c. Electronic parts with different package or surface plating/finish than that ordered e.g., blacktopped components with evidence of sanding and remarking; wrong lead finish; marking for tin finish, actual finish gold.
- d. Electronic parts which have not completed the Original Component Manufacturer's (OCM)'s full production and test flow, but are represented as such.

4.0 REQUIREMENTS

4.1 General Requirements:

In addition to maintaining a quality management system acceptable to ECDATA.COM, the Seller shall develop and maintain documented processes for control of electronic components. These processes shall include supplier management and approvals, procurement, inspection, test/evaluation, segregation, reporting, and disposition of suspect or confirmed counterfeit electronic components. Seller shall maintain supply chain traceability and authenticity of all electronic components through all supply chain operations. The Seller shall employ counterfeit risk mitigation processes commensurate with the risk associated with the application and ensure the quality and authenticity of delivered product.

The Seller shall ensure that counterfeit electronic components are not delivered to ECDATA.COM. Seller shall only purchase products to be incorporated into ECDATA.COM product or delivered to ECDATA.COM from the Original Component Manufacturer (OCM), Original Equipment Manufacturer (OEM), or an OEM/OCM authorized Franchised distributor.

4.2 Counterfeit Electronic Parts Risk Mitigation Process

The Seller shall develop and implement a counterfeit electronic parts risk mitigation process that documents the methods used for avoidance, detection, risk mitigation, disposition, and reporting of counterfeit electronic parts. In addition, the Seller shall have documented processes for purchasing, verification of purchased product, in process investigation, and material control.

<p>SUBJECT</p> <p>COUNTERFEIT AVOIDANCE PROCEDURE</p>	<p>Procedure No. 1.0</p> <p>Revision</p> <p>Effective Date: March 27, 2017</p> <p>Supersedes Rev: Date: March 27, 2017</p> <p>Page: 5 of 12</p>
---	---

4.3 Procurement Process:

The Seller shall:

- a. Document initial and maintenance assessment of all sources of supply for electronic parts to determine risk of counterfeits. Review of supplier performance data, audits, surveys, product alerts may be included as assessment activities;
- b. Develop and maintain a documented list of approved sources. Seller's documented source approval process shall include the criteria required for approval, the scope of the approval, performance evaluation, training of supplier inspection personnel and duration of the approval. The approved source list shall indicate OEM/OCM authorized distributors and franchised distributors.
- c. Provide supply chain traceability to the OEM/OCM through all of the supply chain intermediaries from the electronic part manufacturer to the direct source of the product for the seller. Supply chain traceability is defined as name and location of all supply chain intermediaries for all procurement lots, and date of all intermediate purchases from the part manufacturer to the direct source of the product for the seller. Supply chain traceability is required for all new purchases of electronic parts, electronic parts in inventory, and electronic parts transferred from other businesses within the organization. In the event that documented supply chain traceability is not obtainable or is incomplete, Seller shall notify ECDATA.COM prior to purchase contract acceptance. Seller shall conduct a documented risk mitigation assessment. Seller shall obtain ECDATA.COM's prior written concurrence for tests and inspections required to demonstrate authenticity of parts procured from suppliers that do not have valid OEM Certificate of Conformance or sufficient records providing unbroken supply chain traceability.

The documented processes shall require records providing supply chain traceability to the OEM/OCM or Aftermarket Manufacturer that identifies the supplier's name and location of all of the supply chain intermediaries for all procurement lots, and the date of all intermediate purchases, from the electronic component OEM to the direct source of the product for the supplier. Supply chain traceability records shall be available for ECDATA.COM review upon request. If this supply chain traceability is not available or is incomplete, Seller shall notify ECDATA.COM prior to purchase contract acceptance.

<p>SUBJECT</p> <p>COUNTERFEIT AVOIDANCE PROCEDURE</p>	<p>Procedure No. 1.0</p> <p>Revision</p> <p>Effective Date: March 27, 2017</p> <p>Supersedes Rev:</p> <p>Date: March 27, 2017</p> <p>Page: 6 of 12</p>
---	--

- d. Ensure that processes are in place to audit compliance to the requirements of this document internally and at sub tier suppliers. Audits shall ensure that quality processes have effectively precluded purchase, acceptance, use and delivery of counterfeit electronic parts and adequately reported, contained and segregated counterfeit electronic parts.

4.4 Seller Flowdown

The Seller shall flowdown all applicable requirements of this document to its suppliers when procuring from other distributors or sources. Distributors or sources that do not have a counterfeit electronic components risk mitigation process compliant to this document shall be assessed by the seller for additional risk for every application of the electronic component. ECDATA.COM reserves the right to review and approve all suppliers' risk mitigation processes

4.5 Verification of Purchased Product Process

For cases when components must be purchased from other than authorized suppliers, the devices shall be verified by the seller, or a qualified third party supplier. This seller or supplier shall have a documented process in place to assure detection of counterfeit electronic components. Examples of verification actions include visual inspection, review of data deliverables to Purchase Order requirements, nondestructive evaluation and destructive testing (e.g., marking permanency, x-ray, x-ray fluorescence, destructive physical analysis (DPA), electrical testing). Seller shall maintain verification records in accordance with contractual record retention requirements.

Seller or Supplier personnel performing inspection and testing or reviewing inspection and test results shall have completed all applicable required training and shall be formally qualified for the specific work they perform. Seller or Supplier shall maintain training records in accordance with contractual record retention requirements.

Acceptance and reject criteria shall be defined for all inspections and tests. Results of each inspection and test performed shall be documented, retained, and traceable to product identification (e.g. date/lot codes, serial number), purchase order invoice and inspection and testing personnel.

<p>SUBJECT</p> <p>COUNTERFEIT AVOIDANCE PROCEDURE</p>	<p>Procedure No. 1.0</p> <p>Revision</p> <p>Effective Date: March 27, 2017</p> <p>Supersedes Rev: Date: March 27, 2017</p> <p>Page: 7 of 12</p>
---	---

4.6 Certificate of Conformance

The Seller shall review and retain copies of the electronic part Manufacturer’s original Certificates of Conformance (CoC).

Manufacturer CoCs shall, at minimum, include the following:

- a. Manufacturer name and address;
- b. Manufacturer’s part number;
- c. Batch identification for the item(s) such as date codes, lot codes, serializations, or other batch identifications;
- d. Signature or stamp with title of seller's authorized personnel signing the certificate;
- e. Certification to testing specification and revision level that parts are certified to.

Where manufacturer’s CoCs are not available, the Seller shall notify ECDATA.COM and provide verification of authenticity.

4.7 Material Control and Disposition

Seller shall prevent nonconforming and excess electronic parts from entering the supply chain under fraudulent circumstances. For suspect counterfeit electronic parts, Seller shall ensure that electronic parts are identified as suspect/counterfeit product and quarantined. For suspect counterfeit electronic parts in storage and installed in product, Seller shall quarantine suspect components and assembled product until properly disposition and notify affected customers. Seller shall have documented processes to preclude returning suspect counterfeit electronic parts to the supply chain, which may include controlled conditions to allow for internal investigation.

4.8 Reporting Process

The Seller shall have documented processes for internal/external reporting of all instances of counterfeit electronic components to ensure adequate notification to affected customers.

- a. Electronic parts represented as upscreened; which have not successfully completed all tests e.g., commercial or industrial grade parts marked as military grade parts

<p>SUBJECT</p> <p>COUNTERFEIT AVOIDANCE PROCEDURE</p>	<p>Procedure No. 1.0</p> <p>Revision</p> <p>Effective Date: March 27, 2017</p> <p>Supersedes Rev:</p> <p>Date: March 27, 2017</p> <p>Page: 8 of 12</p>
---	--

- b. Electronic parts with modified labeling or markings that misrepresent the form, fit, function, or part class e.g., Top marking doesn't match bottom marking, varied markings; C of C country doesn't match parts; missing trademark logo and date stamp incorrect; date code after part was discontinued; shadow of previous marking evident; marking didn't match known good part.
- c. Electronic parts scrapped by the OEM and subsequently sold as compliant
- d. Electronic parts which have been refinished, upscreened, or uprated and have been identified as such, are not considered counterfeit.

4.9 Unauthorized/Independent Distributor

Distributors who are neither authorized nor franchised by the original component manufacturer for the parts they sell.

4.10 Upscreening

Additional testing performed on electronic parts to increase confidence in reliability, and to evaluate the lot by discarding defective parts or rejecting the lot. Examples of upscreen testing are Particle Impact Noise Detection (PIND) testing, burn-in, temperature cycling and Radiation Hardness Assurance testing, etc.

4.11 Related Terms

ERAI (Electronic Resellers Association International): A privately held global trade association charged with monitoring, investigating, reporting, and mediating issues affecting the global supply chain of electronics, including counterfeit and substandard electronic components sales.

GIDEP (GOVERNMENT-INDUSTRY DATA EXCHANGE PROGRAM): A cooperative activity between Government and Industry chartered to share technical information essential during all phases of the life cycle of systems, facilities, and equipment.

<p>SUBJECT</p> <p>COUNTERFEIT AVOIDANCE PROCEDURE</p>	<p>Procedure No. 1.0</p> <p>Revision</p> <p>Effective Date: March 27, 2017</p> <p>Supersedes Rev:</p> <p>Date: March 27, 2017</p> <p>Page: 9 of 12</p>
---	--

IDEA (Independent Distributors of Electronics Association): A non-profit trade association representing Independent Distributors who have committed to adhere to prescribed quality and ethical standards. The stated purpose of IDEA is to promote the independent distribution industry through media advocacy; to improve the quality of products and services through a quality certification program, educational seminars and conferences; and to promote the study, development, and implementation of techniques and methods to improve the business of Independent Distributors.

5.0 **OBSOLESCENCE MANAGEMENT RESPONSIBILITIES**

In an effort to further reduce the risk of receiving counterfeit electronic parts, it is the practice of ECDATA.COM to institute obsolescence management practices, where feasible, throughout the life cycle of all our products. These practices include, but not limited to, Diminishing Manufacturing sources and Material Shortages (DMSMS) plans, specific obsolescence management work break down structure (WBS) requirements for mature products and their parts management and the end of life (EOL)/life cycle management (LCM) plans.

6.0 **CONTROL AND DISPOSITION OF COUNTERFEIT OR SUSPECT COUNTERFEIT ELECTRONIC PARTS**

6.1 **Standard**

Any parts determined to be counterfeit or suspect counterfeit electronic parts, and/or product containing such parts, shall be properly identified, controlled, and dispositioned to prevent unintended use or entry into the supply chain.

6.2 **Disposition**

Any parts determined to be counterfeit or suspect counterfeit electronic parts, and/or products containing such parts, will be quarantined in a segregated holding area by ECDATA.COM to prevent unintended use or entry into the supply chain. In order to eliminate the proliferation of counterfeit electronic parts, any such parts will not be returned to the supplier. ECDATA.COM shall consult with the customer and, in cases where an investigation and/or prosecution is ongoing, appropriate law enforcement authorities, regarding the timing and method of final disposition of such parts.

<p>SUBJECT</p> <p>COUNTERFEIT AVOIDANCE PROCEDURE</p>	<p>Procedure No. 1.0</p> <p>Revision</p> <p>Effective Date: March 27, 2017</p> <p>Supersedes Rev:</p> <p>Date: March 27, 2017</p> <p>Page: 10 of 12</p>
---	---

6.3 Additional Testing for Suspect Counterfeit Electronic Parts

When necessary to confirm authenticity, parts determined to be suspect counterfeit electronic parts will be verified by a third party testing facility. Costs associated with such testing shall be borne by the supplier, pursuant to the terms of the relevant purchasing order or contract.

6.4 Preclude Original Use

Any parts ultimately determined to be counterfeit or suspect counterfeit electronic parts, and/or products containing such parts, must be processed in a manner that will ensure the part or product will not be used as originally intended. The part or product must be destroyed, altered in a manner preventing its intended use, or be marked in a permanent manner to ensure detection if introduced for further processing. After the part or product has been altered/marked, it may be used for training, furnished to a Government agency or third-party testing facility, or disposed of through other means. However, any parts determined to be counterfeit or suspect counterfeit electronic parts will not be returned to the supplier.

6.5 GIDEP Notification

If ECDATA.COM becomes aware, or has reason to suspect that any end item, component, part, or material contained in supplies purchased by the Department of Defense, or purchased by ECDATA.COM for delivery to, or on behalf of the Department of Defense, contains counterfeit electronic parts or suspect counterfeit electronic parts, ECDATA.COM is required to report in writing, within 60 days, to appropriate Government authorities and the Government-Industry Data Exchange Program (GIDEP). In order to abolish the proliferation of counterfeit electronic parts, it is ECDATA.COM policy to also notify appropriate Government authorities and GIDEP in cases where ECDATA.COM becomes aware of counterfeit or suspect counterfeit electronic parts supplied to ECDATA.COM for use in any U.S. government contract.

Where there is credible evidence, in cases involving counterfeit or suspect counterfeit electronic parts, of a violation of Federal criminal law involving fraud, conflict of interest, bribery or gratuity, or a violation of the civil False Claims Act in connection with Government contracts, the legal department shall be consulted and any additional disclosures to the Government, as may be required under FAR 3.1001 and FAR 52.203-13, shall be made.

COUNTERFEIT AVOIDANCE PROCEDURE	Procedure No. 1.0 Revision Effective Date: March 27, 2017 Supersedes Rev: Date: March 27, 2017 Page: 11 of 12
---------------------------------	--

6.6 Records

Records of counterfeit or suspect counterfeit electronic parts, and/or products containing such parts and any actions taken to disposition such parts or products, are Quality Records and shall be maintained in accordance with ECDATA.COM Records Management Policy.

6.7 Responsibilities

All personnel are responsible for reporting counterfeit or suspect counterfeit electronic parts, and/or products containing such parts.

7.0 GENERAL

7.1 REVISION HISTORY

Revision	Supersedes Rev/Date	Author(s)	Comments
1.0 03/15/17	New	R Barger	New Quality Procedure

Signed: Richard O Barger

<p>COUNTERFEIT AVOIDANCE PROCEDURE</p> <p>REVISION HISTORY</p>	<p>Procedure No. 1.0</p> <p>Revision</p> <p>Effective Date: March 27, 2017</p> <p>Supersedes Rev:</p> <p>Date: March 27, 2017</p> <p>Page: 12 of 12</p>
--	---

THIS PAGE INTENTENALLY LEFT BLANK