COUNTERFEIT MATERIAL AND MALWARE AVOIDANCE PROCESS REQUIREMENTS

REVISION HISTORY

- Revision 7 replaces revision 6 dated 04/09/20.
    - This revision clarifies Requirement 6.2 and adds a Note referencing Quality Note AW.
- The applicable revision of this document is determined by:
    - The revision specified on the purchase order, or
    - The revision in effect at the time of the purchase order if no revision is listed on the purchase order.

REQUIREMENTS

1. Seller shall maintain a Counterfeit Item risk mitigation process internally and with its Sellers using SAE AS5553 and AS6174 as guidelines.

    1.1. Seller shall flow down to, and ensure compliance with the requirements of this Q-Note by, lower tier Sellers providing items for delivery to ESAero under this order.

    1.2. Seller shall provide evidence of the Seller's risk mitigation process to the ESAero Quality Team upon request.

2. Seller and Seller's sub-tier suppliers that are allowed access to the US Government Industry Data Exchange Program (GIDEP) shall participate in monitoring GIDEP reports and the Seller shall act on GIDEP reports that affect product delivered to ESAero .

    2.1. The Seller shall issue a GIDEP report when suspect or confirmed counterfeit item(s) associated with this Purchase Order are discovered and ensure suspect counterfeit items are not delivered to ESAero .

3. Seller shall immediately notify ESAero with the pertinent facts if the Seller becomes aware or suspects that items delivered in accordance with the ESAero Purchase Order are or contain suspect or confirmed counterfeit items.

4. Seller shall purchase material directly from the Original Equipment Manufacturer (OEM), Original Component Manufacturer (OCM) (collectively, the Original Manufacturer (OM)) or an authorized OM reseller or distributor (collectively, an Authorized Distributor).

    4.1. Seller shall obtain documentation and retain all documentation required to fully trace the distribution and sale of the goods delivered hereunder back to the relevant OM, and, on request of ESAero , shall provide such authenticating documentation.

5. If items required to satisfy this Purchase Order cannot be procured from the OEM, OCM or an OM's Authorized Distributors, the Seller shall obtain written approval from ESAero .

    5.1. The Seller shall present complete and compelling support for any request to procure from sources other than the OEM, OCM or their OM's Authorized Distributors and include in the request all actions completed to ensure the parts thus procured are not Counterfeit Items. Actions may include testing in accordance with Quality Note GP.

5.1.1. If authentication testing has not yet been performed, the Seller shall submit an authentication test plan to ESAero and obtain written approval for the plan prior to starting authentication testing.

5.1.2. If authentication testing has already been performed, the seller shall submit the authentication data to ESAero and obtain written approval prior to part use.

5.2. The supporting documentation shall include:

- Results of authentication test and analysis conducted
- Traceability with identification of all supply chain intermediaries wherever such traceability exists.
- Identification of and traceability to the source for any remarked or resurfaced material.

5.3. The Seller shall segregate and provide traceability identifiers (i.e. Date Code / Lot Code, Serial number) for all items delivered to ESAero which contain an item procured from sources other than OEM, OCM or their Authorized Distributors.

5.4. The Seller shall retain test samples as part of the quality record associated with this Purchase Order.

6. Seller shall maintain the following internal processes to control and prevent malware, defined as viruses, malicious code, Trojan horse, worm, time bomb, self-help code, back door, or other software code or routine designed to: (a) damage, destroy or alter any software or hardware; (b) reveal, damage, destroy, or alter any data; (c) disable any computer program automatically; or (d) permit unauthorized access to any software or hardware:

6.1. Seller shall maintain a malware management process for the underlying manufacturing information systems used in building the electronic assembly. This process shall consist of continuously monitoring the manufacturing information systems to ensure absence of malware, using up-to-date commercially available anti-virus software. The Seller shall maintain evidence of the continuous monitoring (include name/version of the anti-virus software, and scanning machine name/serial number)

6.2. For deliverable assemblies that contain only Commercial-of-the-Shelf (COTS) software or Free and Open Source Software (FOSS) including commercially available operating systems (e.g., Windows, Linux, Mac, and VxWorks), the Seller shall implement a process of scanning these assemblies to ensure that they are free of malware, using up-to-date commercially available anti-virus software. The Seller shall maintain evidence of the scan occurrences (include date of scan, assembly part number, name/version of the anti-virus software, and scanning machine name/serial number).

6.3. Seller shall immediately notify ESAero with the pertinent facts if the Seller becomes aware or suspects that assemblies delivered in accordance with the ESAero Purchase Order contain any malware.

6.4. Seller shall provide evidence of these two processes to ESAero upon request.

DATA SUBMISSION SUMMARY

- Seller to deliver the following data to ESAero for ESAero Approval:
  - Supporting documentation to procure from sources other than the OEM, OCM or their Authorized Distributors as specified in paragraph 5 herein.
- Seller to deliver the following data to ESAero for information as required by this document:
  - Evidence of the Seller's risk mitigation process, if requested.
  - Evidence of the Seller's malware management and malware scanning process, if requested.
  - Evidence of product traceability from the OEM/OCM, if requested.
  - Notification to ESAero with the pertinent facts if the Seller becomes aware or suspects that items delivered in accordance with the ESAero Purchase Order are or contain suspect or confirmed counterfeit items.
  - Notification to ESAero with the pertinent facts if the Seller becomes aware or suspects that assemblies delivered in accordance with the ESAero Purchase Order contain any malware.

NOTES

- “Counterfeit Item” is defined to include, but is not limited to:
  - An item that is an illegal or an unauthorized copy or substitute of an Original Equipment Manufacturer (“OEM”) or Original Component Manufacturer (“OCM”) item.
  - An item that does not contain the proper external or internal materials or components required by the OEM or OCM or that is not constructed in accordance with OEM or OCM design, but is represented as such.
  - An item or component that is used, refurbished or reclaimed but the Seller represents it as being a new item.
  - An item that has not successfully passed all OEM or OCM required testing, verification, screening and quality control but the Seller represents as having met or passed such requirements.
  - An item with a label or other marking intended, or reasonably likely, to mislead a reasonable person into believing a non-OEM or OCM item is a genuine OEM or OCM item when it is not.
- “Authorized Distributor” is defined as a distributor with which the OM has a contractual agreement to stock, repackage, sell and distribute its product lines. Authorized Distributors normally offer the material for sale with full manufacturer flow-through warranty.
- Section 6 of this Quality Note is not applicable for hardware that does not contain software, firmware or microprocessor capability.
- For deliverable assemblies containing non-COTS/non-FOSS software or COTS/FOSS software incorporated into custom software refer to Quality Note AW for software assurance requirements.