



## **Federal Electronics, Inc. Supplier Terms and Conditions**

These standard terms and conditions apply when an override agreement has not been formally negotiated and agreed to by both parties.

- All products must be delivered with a Certificate of Compliance, Supplier Inspection Report, Lot ID and adhere to Federal Electronics SOP PR0013.
- For suppliers of custom fabs, supplier must adhere to Federal Electronics SOP PR0010. Current revisions of these SOPs can be found on the Federal Electronics Supplier Portal using a special access URL.
- A copy of Original Manufacturer's C of C including Part Number, stating all tin plating or tin solder processes contain no less than 3% lead composition and that components are in compliance with DFARS 252.225-7009.
- If this PO or RFQ references any Mil-spec parts, it is supplier's responsibility to ensure parts are manufactured by an approved source listed in the DoD Qualified Products Database if applicable.
- Federal Electronics conforms with ITAR regulations requiring Vendor compliance. PO or RFQ may reference data subject to U.S. Government Requirements re: (EAR) 15 CFR Parts 730-99; (ITAR) Parts 120-1330 therefore Supplier will secure any data transfer in its own name.
- Federal Electronics is an EEO employer.
- If this purchase order or RFQ is a rated order certified for national defense use, then the Supplier shall follow all requirements of the Defense Priorities and Allocations System regulation (15 CFR Part 700).
- Federal Electronic requires that all Suppliers utilize the Federal Electronics UPS account for transportation charges when authorized. Multiple items must be consolidated into a single shipment. Supplier may not use a declared value on any shipment to Federal Electronics. In the event that a Supplier utilizes a Declared Value, that amount will be deducted from future payments for the products received.
- Please insure all shipments are delivered to Federal Electronics no more than three days early, zero days late.
- Age controlled material must have a minimum of 8 months of its remaining shelf life at the time of shipment. Each shipment is to be identified with the date of manufacture/date of expiration.
- Firmed Orders Are For Planning Purposes Only. Only Accept Released Orders As A Commitment For Purchase And Payment Of Materials And Services.



- DFARS Cybersecurity Flowdowns
  - The following clauses are required for any products identified as “-ITAR” or “-CUI”.
  - 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (12/2019) (Applicable in subcontracts for operationally critical support or for which subcontract performance will involve covered defense information, including subcontracts for commercial items, without alteration, except to identify the parties. When applicable, this clause, in its entirety, is hereby flowed down as if the language of the clause is contained within this document.) SUBCONTRACTORS NOT COMPLIANT WITH DFARS 252.204-7012 SHALL NOT STORE, SEND, RECEIVE OR CREATE ANY COVERED DEFENSE INFORMATION (CDI) OR CONTROLLED UNCLASSIFIED INFORMATION (CUI) ON SUBCONTRACTOR’S COVERED INFORMATION SYSTEMS INCLUDING DIGITAL PHOTOGRAPHS OR COPIES. SUBCONTRACTORS SHALL REPORT ANY BREACH OF DFARS REQUIREMENT TO BUYER WITHIN TWENTY-FOUR (24) HOURS OF ANY BREACH OR POTENTIAL BREACH OF THIS PROTOCOL. Subcontractor must notify Contractor when submitting a request to vary from a NIST SP 800- 171 security requirement, in accordance with paragraph (b)(2)(ii)(B) of this clause. Subcontractor must provide the incident report number, automatically assigned by DoD, to the Contractor as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause
  - 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements (Applicable for any subcontractor that has access to, processes, stores, or transmits Controlled Unclassified Information, CUI. This clause must be flowed down to all subcontractors at all tiers)
  - 252.204-7020 NIST SP 800-171 Assessment Requirements (Applicable for any subcontractor that has access to, processes, stores, or transmits Controlled Unclassified Information, CUI. This clause must be flowed down to all subcontractors at all tiers)
  - 252.204-7021 Cybersecurity Maturity Model Certification Requirements (Applicable for any subcontractor that has access to, processes, stores, or transmits Controlled Unclassified Information, CUI. This clause must be flowed down to all subcontractors at all tiers)
- By accepting this PO or processing this RFQ the vendor certifies that they are in compliance with the terms and conditions listed above.