M&S Machining, Inc. Purchase Order Quality Flow Downs

Your involvement directly contributes to the conformity of all products shown on this order. Your commitment to quality, good business ethics, product safety and compliance with all PO requirements, including the requirements within this flow down are important to the overall end user satisfaction.

Record retention- Supplier agrees to retain all records associated with this PO for a minimum of 7 years unless otherwise stated in the contract. Records shall be maintained and made available in a timely manner to M&S Machining, its customers, and regulatory authorities upon request.

Flow down of requirements- when work related to this PO is outsourced to a sub-tier, the supplier agrees to flow down the appropriate requirements to their sub-tier. The appropriate requirements include but are not limited to key characteristics, control of special processes, record retention, flow down of quality system requirements, these M&S flow downs and any other requirements on the M&S purchase order, including M&S customer requirements/flow downs. The supplier also agrees to verification of outsourced work to sub-tiers as well as control and monitoring of external providers.

Qualification of personnel- Supplier is responsible for maintaining training records of employees, and maintaining all special process certifications (I.e. welding, non-destructive inspection, etc).

Supplier process change control- The supplier agrees to obtain M&S Machining approval to either:

A. Relocation of work to another production facility
B. Changing the design, manufacturing processes, products or services, or suppliers.

An analysis shall be performed, documented and included with any request for change.

Notification of nonconformities- Supplier agrees to notify M&S Machining of any nonconforming product that requires disposition other than rework. Suppliers are not granted the authority to process (Use as is, or repair).

Suppliers are requested to hold certification to AS9100, at a minimum maintain a Quality system that meets ISO 9001 requirements. Compliance is subject to audit by M&S Machining.

Suppliers are requested to have Counterfeit Prevention measures in place in compliance with AS9100 standards.

If M&S flows down customer designated or approved external provider, they are required to be used (such as special processes) M&S will notify you in the PO.

If test specimens for design approval, inspection/verification, investigation or auditing is required, M&S will notify you in the PO.

FARS Requirements:

This purchase agreement incorporates one or more clauses by reference, with the same force and effect as if they were in full test, and are as follows:

52.203-19 – Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements
52.204-21 – Basic Safeguarding of Covered Contractor Information Systems
252.204-7009 – Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information
252.204-7012 – Safeguarding Covered Defense Information and Cyber Incident Reporting
252.204-7015 – Notice of Authorized Disclosure of Information for Litigation Support
52.222-21 – Prohibition of Segregated Facilities
52.226-26 – Contractors Performing Private Security Functions outside the United States.
52.226-36 – Affirmative Action for Handicapped Workers (Applies to contracts over $2,500).
52.223-18 – Encouraging Contractor Policies to Ban Text Messaging While Driving
52.225-13 – Restrictions on Certain Foreign Purchases
252.225-7007 – Prohibition on Acquisition of United States Munitions List Items from Communist Chinese Military Companies
252.227-7016 – Rights in Bid or Proposal Information
252.227-7037 – Validation of Restrictive Markings on Technical Data
52.232-40 – Providing Accelerated Payments to Small Business Subcontractors
252.244-7000 – Subcontracts for Commercial Items
252.246-7003 – Notification of Potential Safety Issues
252.225-7048 – Export Controlled Items
52.222-26 – Equal Opportunity
52.225-20 – Prohibition on Conducting Restricted Business Operations in Sudan--Certification
52.225-25 – Prohibition on Contracting with Entities Engaging in Certain Activities or Transactions Relating to Iran – Representation and Certifications.
52.233-3 – Protest after Award
52.232-40 – Providing Accelerated Payments to Small Business Subcontractors
52.233-4 – Applicable Law for Breach of Contract Claim
52.244-6 – Subcontracts for Commercial Items
52.203-13 – Contractor Code of Business Ethics and Conduct
52.203-15 – Whistleblower Protections Under the American Recovery and Reinvestment Act of 2009
52.219-8 – Utilization of Small Business Concerns
52.222-40 – Notification of Employee Rights Under the National Labor Relations Act
52.224-3 – Privacy Training
52.225-26 – Contractors Performing Private Security Functions Outside the United States
52.253-1 – Computer Generated Forms

52.222-19 – Child Labor (Applies to to contracts for supplies exceeding the micro-purchase threshold)
52.222-35 – Equal Employment for Workers with Disabilities (Applies to contracts over $15,000, unless the work performed is performed outside the United States)
52.222-36 – Equal Employment for Workers with Disabilities (Applies to contracts over $15,000, unless the work is to be performed outside the United States by employees recruited outside the United States)
52.222-37 – Employment Reports on Veterans (Applies to contracts of $150,000 or more)
52.222-50 – Combating Trafficking in Persons (Applies to all solicitations and contracts)
52.222-55 – Minimum Wages under Executive Order 13658 (Applies when 52.222-6 or 52.222-41 are in the contract and performance in whole or in part is in the United States (the 50 States and the District of Columbia).
52.222-62 – Paid Sick Leave under Executive Order 13706 (Applies when 52.222-6 or 52.222-41 are in the contract and performance in whole or in part is in the United States (the 50 States and the District of Columbia.))
52.247-64 – Preference for Privately Owned U.S.-Flag Commercial Vessels (Applies to transported by ocean vessels (except for the types of subcontracts listed at 47.504(d).)
52.204-21 – Basic Safeguarding of Covered Contractor Information Systems (Applies to contracts when the contractor of a subcontractor at any tier may have Federal contract information residing in or transiting through its information system).
52.209-6 – Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment (Applies to contracts over $35,000).

LIMITATIONS ON THE USE OR DISCLOSURE OF THIRD-PARTY

CONTRACTOR REPORTED CYBER INCIDENT INFORMATION (OCT 2016)

(a) Definitions. As used in this clause—

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

“Controlled technical information” means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

“Covered defense information” means unclassified controlled technical information or other information (as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html) that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—

(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or

(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.

“Cyber incident” means actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

“Information system” means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

“Media” means physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.

“Technical information” means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data-Noncommercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

(b) Restrictions. The Contractor agrees that the following conditions apply to any information it receives or creates in the performance of this contract that is information obtained from a third-party’s reporting of a cyber incident pursuant to DFARS clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (or derived from such information obtained under that clause):

(1) The Contractor shall access and use the information only for the purpose of furnishing advice or technical assistance directly to the Government in support of the Government's activities related to clause 252.204-7012, and shall not be used for any other purpose.

(2) The Contractor shall protect the information against unauthorized release or disclosure.

(3) The Contractor shall ensure that its employees are subject to use and non-disclosure obligations consistent with this clause prior to the employees being provided access to or use of the information.

(4) The third-party contractor that reported the cyber incident is a third-party beneficiary of the non-disclosure agreement between the Government and Contractor, as required by paragraph (b)(3) of this clause.

(5) A breach of these obligations or restrictions may subject the Contractor to—

(i) Criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and other appropriate remedies by the United States; and

(ii) Civil actions for damages and other appropriate remedies by the third party that reported the cyber incident, as a third party beneficiary of this clause.

(c) Subcontracts. The Contractor shall include this clause, including this paragraph (c), in subcontracts, or similar contractual instruments, for services that include support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items, without alteration, except to identify the parties.

SUPPLIER CONDUCT PRINCIPLES

SELLER commits itself to conduct its business activities in a fair, honest, responsible, ethical, and lawful manner and in strict adherence to all applicable laws and regulations governing the ethical and legal conduct of business organizations. Supplier Conduct Principles are available in form KOG-DIR-0038 at www.kongsberg.com. The Supplier Conduct Principles are an integral part of the Contract, and SELLER is expected to comply with or actively pursue compliance with these principles. SELLER shall upon written request from BUYER always be obliged to: (i) document compliance with the requirements set forth above; and (ii) allow BUYER, BUYER's customer, or a third party appointed by BUYER or BUYER's customer the right to conduct such audits as it finds necessary to verify compliance with the requirements of this clause. For the avoidance of doubt the audit rights shall include: (a) unrestricted access to all production sites and premises; and (b) the right to communicate with and interview employees and other personnel; and (c) the right to review pertinent documentation or any other relevant material. SELLER shall ensure that any of SELLER's lower tier suppliers may also be subject to such audits as described above. The Parties shall carry their own costs incurred in relation to performance of such documentation and audit.