FLOWDOWN CLAUSES APPLICABLE TO PURCHASE ORDERS INVOLVING CONTROLLED UNCLASSIFIED INFORMATION (CUI)

When goods or services furnished by the Seller to a TE Entity for use in connection with a U.S. Government contract or subcontract and contain Controlled Unclassified Information (CUI), which for the purposes of contracts between Seller and a TE Entity includes Covered Defense Information (CDI), in addition to the TE Global Terms and Conditions of Purchase, certain clauses shall apply, as required by the terms of the prime contract, or by operation of law or regulation. A TE Entity is defined as an entity within the TE Connectivity Ltd. family of companies, which shall include all direct and indirect subsidiaries and affiliates of TE Connectivity Ltd. (also collectively referred to as "TE").

The following clauses from the Federal Acquisition Regulation ("FAR") and the Defense Federal Acquisition Regulation Supplement ("DFARS") are incorporated into the Purchase Order (the "Order") by reference where applicable and form a part of the terms and conditions of the Order. The full text of all clauses incorporated by reference are available at: http://www.acquisition.gov/. Seller agrees to flow down all applicable FAR and DFARS clauses to lower-tier subcontractors.

In all clauses listed herein, the terms "Government," "Contracting Officer", and "Contractor" shall be revised to suitably identify the contracting parties herein and affect the proper intent of the clause or provision. It is intended that the referenced clauses shall apply to Seller in such manner as is necessary to reflect the position of Seller as a subcontractor or supplier to a TE Entity, to ensure Seller's obligations to a TE Entity and to the U.S. Government, and to enable a TE Entity to meet its obligations under a U.S. Government prime contract or subcontract.

TE is committed to compliance with U.S. Government requirements regarding cybersecurity and cyber incident reporting. This includes implementing adequate security requirements outlined in NIST SP 800-171, and in the applicable FAR and DFARS clauses as set forth below.

TE's safeguarding obligations extend not only to information received from the U.S. Government or a U.S. Government contractor or subcontractor during contract performance, but also to any CUI that is collected, developed, received, used, or stored by or on behalf of TE in support of the performance of a U.S. Government contract.

FAR 52.204-21	Basic Safeguarding of Covered Contractor Information Systems.	(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.
DFARS 252.204-7008	Compliance with Safeguarding Covered Defense Information Controls.	By submission of its offer, the Seller represents that it will implement the security requirements specified by National Institute of Standards and Technology Special Publication 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017.
DFARS 252.204-7009	Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.	(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph (c), in all subcontracts for services that includes support for the Government's activities related to safeguarding covered defense information and cyber incident reporting, including subcontracts for commercial items.
DFARS 252.204-7012	Safeguarding covered defense information and cyber incident reporting	(m) Subcontracts. The Contractor shall - (1) Include this clause, including this paragraph (m), in subcontracts, or similar contractual instruments, 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. The Contractor shall determine if the information required for subcontractor performance retains its identity as covered defense information and will require protection under this clause, and, if necessary, consult with the Contracting Officer; and (2) Require subcontractors to - (i) Notify the prime Contractor (or next higher-tier subcontractor) when submitting a request to vary from a NIST SP 800-171 security requirement to the Contracting Officer, in accordance with paragraph (b)(2)(ii)(B) of this clause; and (ii) Provide the incident report number, automatically assigned by DoD, to the prime Contractor (or next higher-tier subcontractor) as soon as practicable, when reporting a cyber incident to DoD as required in paragraph (c) of this clause.
DFARS 252.204-7014	Limitations on the Use or Disclosure of Information by Litigation Support Contractors.	(e) Flowdown. Include the substance of this clause, including this paragraph (e), in all subcontracts, including subcontracts for commercial items.
DFARS 252.204-7020	NIST SP 800-171 DoD Assessment Requirements.	(g) Subcontracts. (1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items). (2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in this link in this clause, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government. (3) If a subcontractor does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800-171 DoD Assessment Methodology, to webptsmh@navy.mil for posting to SPRS along with the information required by paragraph (d) of this clause.
DFARS 252.204-7021	Cybersecurity Maturity Model Certification Requirement.	(c) Subcontracts. The Contractor shall— (1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding commercially available off-the-shelf items; and (2) Prior to awarding to a subcontractor, ensure that the subcontractor has a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the subcontractor.