QC200 - Chase Defense PO Flowdowns of FAR and DFARS Clauses

Supplier is responsible for all applicable flowdowns. Please contact 757-245-2800 or send an email to info@chasedefense.com if there are any questions or issues with compliance and applicability. When the items furnished are for use in connection with a U.S. Government prime contract or subcontract, the following applicable provisions shall be considered a part of this purchase order.

Order of precedence – Should there be a conflict between any parts of this purchase order and referenced documents/requirements, the purchase order itself and any revisions or modifications to the purchase order shall take precedence. However, the Seller shall immediately notify Chase Defense in writing of any inconsistencies or conflicts that have been observed. The general order of precedence beyond the purchase order is as follows:
1) Chase Defense QC Notes and Terms & Conditions
2) DFARS and FAR clauses, and any other regulations referenced by the purchase order
3) Drawings
4) Other referenced documents/attachments
5) Specifications

For the purchase of commercial items under purchase orders placed in support of a U.S. Government contract or subcontract, the only applicable FAR and DFARS clauses are in **bold**. In all the clauses below, and unless the text in these clauses clearly reserves rights to the Government only, any references to "Government" shall be interpreted to refer to the Buyer, and "Contractor" referring to the Seller under this purchase order.

Federal Acquisition Regulations (FAR)
https://www.acquisition.gov/browse/index/far

Gratuities 52.203-3
Covenant Against Contingent Fees 52.203-5
Restrictions on Subcontractor Sales to the Government 52.203-6
Price or Fee Adjustment for Illegal or Improper Activity 52.203-10
Contractor Employer Whistleblower Rights and Requirement to Inform Employees of Whistleblower Rights 52.203-17
Security Requirements 52.204-2
Personal Identity Verification of Contractor Personnel 52.204-9
Reporting Executive Compensation and First-Tier Subcontract Awards 52.204-10
Basic Safeguarding of Covered Contractor Information Systems 52.204-21
Material Requirements 52.211-5
Defense Priority and Allocation Requirements 52.211-15
Contract Terms Required to Implement Statutes or Executive Orders – Commercial Items 52.212-5
Integrity of Unit Prices 52.215-14
Utilization of Small Business Concerns 52.219-8
Notice to Government of Labor Disputes 52.222-1
Prohibition of Segregated Facilities 52.222-21
Equal Opportunity 52.222-26
Service Contract Labor Standards 52.222-41
Combating Trafficking in Persons 52.222-50
Exemption from Application of the Service Contract Labor Standards to Contracts for Maintenance, Calibration, or Repair of Certain Equipment – Requirements 52.222-51
Exemption From Application of the Service Labor Standards to Contracts for Certain Services — Requirements 52.222-53
Hazardous Material Identification and Material Safety Data 52.223-3
Drug-Free Workplace 52.223-6
Notice of Radioactive Materials (''Government means ''Government and Buyer'') 52.223-7

Ozone-Depleting Substances and High Global Warming Potential Hydrofluorocarbons 52.223-11
Encouraging Contractor Policies to Ban Text Messaging While Driving 52.223-18
Privacy Act Notification 52.224-1
Privacy Act 52.224-2
Buy-America Act-Supplies 52.225-1
Duty-free Entry 52.225-8
Restrictions on Certain Foreign Purchases 52.225-13
Authorization and Consent — Alternate 1 52.227-1
Refund of Royalties 52.227-9
Filing of Patent Applications — Classified Subject Matter 52.227-10
Patent Rights – Ownership by the Contractor 52.227-11
Patent Rights – Ownership by the Government 52.227-13
Rights in Data — General (Not applicable under Department of Defense procurements) 52.227-14
Commercial Computer Software License 52.227-19
Rights in Data – SBIR Program 52.227-20
Worker's Compensation Insurance (Defense Base Act) 52.228-3
Workers Compensation and War-Hazard Insurance Overseas 52.228-4
Insurance — Work on a Government Installation 52.228-5
Industrial Resources Developed Under Defense Production Act Title III 52.234-1
Accident Prevention 52.236-13
Changes – Fixed-Price 52.243-1
Competition in Subcontracting 52.244-5
Subcontracts for Commercial Items 52.244-6
Government Property 52.245-1
Government Property Installation Operation Service 52.245-2
Inspection of Supplies — Fixed Price 52.246-2
Inspection of Supplies — Cost Reimbursement 52.246-3
Inspection of Services — Fixed Price 52.246-4
Preference for U.S. Flag Air Carriers 52.247-63
Preference for Privately Owned U.S. Flag Commercial Vessels 52.247-64
Termination for Convenience of the Government (Fixed Price) ''Government'' shall mean ''Buyer.'' 52.249-2

<u>Orders Over $10,000 Shall Also Include the Following:</u>
Notification of Employee Rights Under the National Labor Relations Act 52.222-40

<u>Orders Over $15,000 Shall Also Include the Following:</u>
Walsh-Healy Public Contracts Act 52.222-20
Equal Opportunity for Workers with Disabilities 52.222-36

<u>Orders Over $25,000 Shall Also Include the Following:</u>
Promoting Excess Food Donations to Nonprofit Organizations 52.226-6

<u>Orders Over $150,000 Shall Also Include the Following:</u>
Anti-Kickback Procedures (less paragraph (c) (1)) 52.203-7
Limitation on Payments to Influence Certain Federal Transactions 52.203-12
Preventing Personal Conflicts of Interest 52.203-16
Equal Opportunity for Veterans 52.222-35
Employment Reports Veterans 52.222-37
Value Engineering 52.248-1
Limitation on Payments to Influence Certain Federal Transactions 52.203-12
Certification and Disclosure Regarding Payments to Influence Certain Federal Transactions (over $150,000) 52.203-11

Certification Regarding Debarment, Suspension, Proposed Debarment and Other Responsibility Matters (over $150,000) 52.209-5
Previous Contracts and Compliance Reports (over $150,000) 52.222-22

Orders Over $700,000 Shall Also Include the Following:
Small Business Subcontracting Plan 52.219-9

Orders Over $750,000 and/or the Applicable Cost or Pricing Data Threshold Shall Also Include the Following:
Audit and Records — Sealed Bidding 52.214-26
Price Reduction for Defective Cost of Pricing Data — Modifications — Sealed Bidding 52.214-27
Subcontractor Cost or Pricing Data — Modifications — Sealed Bidding 52.214-28
Audit and Records – Negotiation (applicable to cost type contracts and contracts requiring certified cost or pricing data submission)
52.215-2
Subcontractor Certified Cost or Pricing Data – Modifications 52.215-13
Pension Adjustments and Asset Reversions 52.215-15
Reversion or Adjustment of Plans for Post-Retirement Benefits Other Than Pensions 52.215-18
Notification of Ownership Changes 52.215-19
Limitations on Pass-Through Charges 52.215-23

Unless Otherwise Exempt Also Include the Following:
Protecting Government Interest when Subcontracting with Contractors Debarred, suspended, or Proposed for Debarment
52.209-6
Price Reduction for Defective Certified Cost or Pricing Data 52.215-10
Price Reduction for Defective Certified Cost or Pricing Data Modifications 52.215-11
Subcontractor Certified Cost or Pricing Data 52.215-12
Subcontractor Certified Cost or Pricing Data Modifications 52.215-13
Requirements for Cost or Pricing Data or Information other than Certified Cost or Pricing Data 52.215-20
Requirements for Cost or Pricing Data or Information other than Certified Cost or Pricing Data — Modifications 52.215-21
Contract Work Hours and Safety Standards – Overtime Compensation 52.222-4
Subcontracts — Labor Standards 52.222-11
Child Labor — Cooperation with Authorities and Remedies 52.222-19
Pre-award On-site Equal Opportunity Compliance Evaluation 52.222-24
Buy American Act — Free Trade Agreements-Israeli Trade Act 52.225-3
Trade Agreements 52.225-5
Contractor Personnel in a Designated Operational Area or Supporting a Diplomatic or Consular Mission Outside the United States 52.225-19
Patent Rights — Ownership by the Government 52.227-13
Cost Accounting Standards — Educational Institution 52.230-5
Earned Value Management System 52.234-4
Change Order Accounting 52.243-6
Notification of Changes 52.243-7

FAR clauses required to be flowed down in their entirety

FAR 52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities.

(a) *Definitions*. As used in this clause—

***Covered article* means any hardware, software, or service that–**

(1)Is developed or provided by a covered entity;

(2)Includes any hardware, software, or service developed or provided in whole or in part by a covered entity; or

(3)Contains components using any hardware or software developed in whole or in part by a covered entity.

***Covered entity* means–**

(1)Kaspersky Lab;

(2)Any successor entity to Kaspersky Lab;

(3)Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4)Any entity of which Kaspersky Lab has a majority ownership.

(b) *Prohibition*. Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from—

(1)Providing any covered article that the Government will use on or after October 1, 2018; and

(2)Using any covered article on or after October 1, 2018, in the development of data or deliverables first produced in the performance of the contract.

(c) *Reporting requirement*.

(1)In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2)The Contractor shall report the following information pursuant to paragraph (c)(1) of this clause:

(i)Within 1 business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; brand; model number (Original Equipment Manufacturer (OEM) number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii)Within 10 business days of submitting the report pursuant to paragraph (c)(1) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered article, any reasons that led to the use or submission of the covered article, and any additional efforts that will be incorporated to prevent future use or submission of covered articles.

(d)Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (d), in all subcontracts, including subcontracts for the acquisition of commercial items.

FAR 52.209-6 Protecting the Government's Interest When Subcontracting With Contractors Debarred, Suspended, or Proposed for Debarment.

(a) Definition. Commercially available off-the-shelf (COTS) item, as used in this clause -

(1) Means any item of supply (including construction material) that is -

(i) A commercial item (as defined in paragraph (1) of the definition in FAR 2.101);

(ii) Sold in substantial quantities in the commercial marketplace; and

(iii) Offered to the Government, under a contract or subcontract at any tier, without modification, in the same form in which it is sold in the commercial marketplace; and

(2) Does not include bulk cargo, as defined in 46 U.S.C. 40102(4), such as agricultural products and petroleum products.

(b) The Government suspends or debars Contractors to protect the Government's interests. Other than a subcontract for a commercially available off-the-shelf item, the Contractor shall not enter into any subcontract, in excess of $35,000 with a Contractor that is debarred, suspended, or proposed for debarment by any executive agency unless there is a compelling reason to do so.

(c) The Contractor shall require each proposed subcontractor whose subcontract will exceed $35,000, other than a subcontractor providing a commercially available off-the-shelf item, to disclose to the Contractor, in writing, whether as of the time of award of the subcontract, the subcontractor, or its principals, is or is not debarred, suspended, or proposed for debarment by the Federal Government.
(d) A corporate officer or a designee of the Contractor shall notify the Contracting Officer, in writing, before entering into a subcontract with a party (other than a subcontractor providing a commercially available off-the-shelf item) that is debarred, suspended, or proposed for debarment (see FAR 9.404 for information on the System for Award Management (SAM) Exclusions). The notice must include the following:
(1) The name of the subcontractor.
(2) The Contractor's knowledge of the reasons for the subcontractor being listed with an exclusion in SAM.
(3) The compelling reason(s) for doing business with the subcontractor notwithstanding its being listed with an exclusion in SAM.
(4) The systems and procedures the Contractor has established to ensure that it is fully protecting the Government's interests when dealing with such subcontractor in view of the specific basis for the party's debarment, suspension, or proposed debarment.
(e) Subcontracts. Unless this is a contract for the acquisition of commercial items, the Contractor shall include the requirements of this clause, including this paragraph (e) (appropriately modified for the identification of the parties), in each subcontract that -
(1) Exceeds $35,000 in value; and
(2) Is not a subcontract for commercially available off-the-shelf items.

FAR 52.225-13 Restrictions on Certain Foreign Purchases.
(a) Except as authorized by the Office of Foreign Assets Control (OFAC) in the Department of the Treasury, the Contractor shall not acquire, for use in the performance of this contract, any supplies or services if any proclamation, Executive order, or statute administered by OFAC, or if OFAC's implementing regulations at 31 CFR chapter V, would prohibit such a transaction by a person subject to the jurisdiction of the United States.
(b) Except as authorized by OFAC, most transactions involving Cuba, Iran, and Sudan are prohibited, as are most imports from Burma or North Korea, into the United States or its outlying areas. Lists of entities and individuals subject to economic sanctions are included in OFAC's List of Specially Designated Nationals and Blocked Persons at http://www.treas.gov/offices/enforcement/ofac/sdn More information about these restrictions, as well as updates, is available in the OFAC's regulations at 31 CFR chapter V and/or on OFAC's Web site at http://www.treas.gov/offices/enforcement/ofac.
(c) The Contractor shall insert this clause, including this paragraph (c), in all subcontracts.

FAR 52.222-21 Prohibition of Segregated Facilities
(a) Definitions. As used in this clause -
Gender identity has the meaning given by the Department of Labor's Office of Federal Contract Compliance Programs, and is found at www.dol.gov/ofccp/LGBT/LGBT_FAQs.html.
Segregated facilities means any waiting rooms, work areas, rest rooms and wash rooms, restaurants and other eating areas, time clocks, locker rooms and other storage or dressing areas, parking lots, drinking fountains, recreation or entertainment areas, transportation, and housing facilities provided for employees, that are segregated by explicit directive or are in fact segregated on the basis of race, color, religion, sex, sexual orientation, gender identity, or national origin because of written or oral policies or employee custom. The term does not include separate or single-user rest rooms or necessary dressing or sleeping areas provided to assure privacy between the sexes.
Sexual orientation has the meaning given by the Department of Labor's Office of Federal Contract Compliance Programs, and is found at www.dol.gov/ofccp/LGBT/LGBT_FAQs.html.
(b) The Contractor agrees that it does not and will not maintain or provide for its employees any segregated facilities at any of its establishments, and that it does not and will not permit its employees to perform their services at any location under its control where segregated facilities are maintained. The Contractor agrees that a breach of this clause is a violation of the Equal Opportunity clause in this contract.

(c) The Contractor shall include this clause in every subcontract and purchase order that is subject to the Equal Opportunity clause of this contract.

FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.

(a) ***Definitions.*** **As used in this clause—**

Covered foreign country **means The People's Republic of China.**

Covered telecommunications equipment or services **means–**

(1)Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities);

(2)For the purpose of public safety, security of Government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities);

(3)Telecommunications or video surveillance services provided by such entities or using such equipment; or

(4)Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Critical technology **means–**

(1)Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2)Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled-

(i)Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii)For reasons relating to regional stability or surreptitious listening;

(3)Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4)Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);

(5)Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or

(6)Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).

Substantial or essential component **means any component necessary for the proper function or performance of a piece of equipment, system, or service.**

(b) ***Prohibition.*** **Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232) prohibits the head of an executive agency on or after August 13, 2019, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception at paragraph (c) of this clause applies or the covered telecommunication equipment or services are covered by a waiver described in Federal Acquisition Regulation 4.2104.**

(c) ***Exceptions.*** **This clause does not prohibit contractors from providing—**

(1)A service that connects to the facilities of a third-party, such as backhaul, roaming, or interconnection arrangements; or

(2)Telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(d)Reporting requirement.

(1)In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information in paragraph (d)(2) of this clause to the Contracting Officer, unless elsewhere in this contract are established procedures for reporting the information; in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil. For indefinite delivery contracts, the Contractor shall report to the Contracting Officer for the indefinite delivery contract and the Contracting Officer(s) for any affected order or, in the case of the Department of Defense, identify both the indefinite delivery contract and any affected orders in the report provided at https://dibnet.dod.mil.

(2)The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause

(i)Within one business day from the date of such identification or notification: the contract number; the order number(s), if applicable; supplier name; supplier unique entity identifier (if known); supplier Commercial and Government Entity (CAGE) code (if known); brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.

(ii)Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of covered telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.

(e) *Subcontracts.* The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

DFARS 252.204-7018 Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services.

(a) Definitions. As used in this clause -

Covered defense telecommunications equipment or services means -

(1) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation, or any subsidiary or affiliate of such entities;

(2) Telecommunications services provided by such entities or using such equipment; or

(3) Telecommunications equipment or services produced or provided by an entity that the Secretary of Defense reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

Covered foreign country means -

(1) The People's Republic of China; or

(2) The Russian Federation.

Covered missions means -

(1) The nuclear deterrence mission of DoD, including with respect to nuclear command, control, and communications, integrated tactical warning and attack assessment, and continuity of Government; or

(2) The homeland defense mission of DoD, including with respect to ballistic missile defense.

"Critical technology" means -

(1) Defense articles or defense services included on the United States Munitions List set forth in the International Traffic in Arms Regulations under subchapter M of chapter I of title 22, Code of Federal Regulations;

(2) Items included on the Commerce Control List set forth in Supplement No. 1 to part 774 of the Export Administration Regulations under subchapter C of chapter VII of title 15, Code of Federal Regulations, and controlled -

(i) Pursuant to multilateral regimes, including for reasons relating to national security, chemical and biological weapons proliferation, nuclear nonproliferation, or missile technology; or

(ii) For reasons relating to regional stability or surreptitious listening;

(3) Specially designed and prepared nuclear equipment, parts and components, materials, software, and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities);

(4) Nuclear facilities, equipment, and material covered by part 110 of title 10, Code of Federal Regulations (relating to export and import of nuclear equipment and material);
(5) Select agents and toxins covered by part 331 of title 7, Code of Federal Regulations, part 121 of title 9 of such Code, or part 73 of title 42 of such Code; or
(6) Emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018 (50 U.S.C. 4817).
Substantial or essential component means any component necessary for the proper function or performance of a piece of equipment, system, or service.
(b) Prohibition. In accordance with section 1656 of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91), the contractor shall not provide to the Government any equipment, system, or service to carry out covered missions that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless the covered defense telecommunication equipment or services are covered by a waiver described in Defense Federal Acquisition Regulation Supplement 204.2104.
(c) Procedures. The Contractor shall review the list of excluded parties in the System for Award Management (SAM) at https://www.sam.gov for entities that are excluded when providing any equipment, system, or service, to carry out covered missions, that uses covered defense telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless a waiver is granted.
(d) Reporting.
(1) In the event the Contractor identifies covered defense telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, the Contractor shall report at https://dibnet.dod.mil the information in paragraph (d)(2) of this clause.
(2) The Contractor shall report the following information pursuant to paragraph (d)(1) of this clause:
(i) Within one business day from the date of such identification or notification: The contract number; the order number(s), if applicable; supplier name; brand; model number (original equipment manufacturer number, manufacturer part number, or wholesaler number); item description; and any readily available information about mitigation actions undertaken or recommended.
(ii) Within 10 business days of submitting the information in paragraph (d)(2)(i) of this clause: Any further available information about mitigation actions undertaken or recommended. In addition, the Contractor shall describe the efforts it undertook to prevent use or submission of a covered defense telecommunications equipment or services, and any additional efforts that will be incorporated to prevent future use or submission of covered telecommunications equipment or services.
(e) Subcontracts. The Contractor shall insert the substance of this clause, including this paragraph (e), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items.

Defense Federal Acquisition Regulation Supplement (DFARS)
https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html

Requirement to Inform Employees of Whistleblower Rights 252.203-7002
Disclosure of Information 252.204-7000
Limitations on the Use of Disclosure of Third-Party Contractor Reported Cyber Incident Information
Safeguarding Covered Defense Information and Cyber Incident Reporting 252.204-7012
Intent to Furnish Precious Metals as Government-Furnished Material 252.208-7000
Item Unique Identification and Valuation 252.211-7003
Pricing of Adjustments 252.215-7000
Restrictions on Employment of Personnel 252.222-7000
Hazard Warning Labels 252.223-7001
Drug-Free Work Force 252.223-7004
Prohibition on Storage and Disposal of Toxic and Hazardous Materials (Alternate) 252.223-7006
Prohibition of Hexavalent Chromium 252.223-7008
Buy American Act – Balance of Payments Certificate 252.225-7000

Buy America Act and Balance of Payments Program 252.225-7001
Qualifying Country Sources as Subcontractors 252.225-7002
Quarterly Reporting of Actual Contract Performance Outside the United States 252.225-7006
Prohibition on Acquisition of United States Munitions List Items from Communist Chinese Military Companies 252.225-7007
Restriction on Acquisition of Specialty Metals 252.225-7008
Restriction on Acquisition of Certain Articles Containing Specialty Metals 252.225-7009
Restriction on Acquisition of Super Computers 252.225-7011
Preference for Certain Domestic Commodities 252.225-7012
Duty-Free Entry 252.225-7013
Restriction on Acquisition of Hand or Measuring Tools 252.225-7015
Restriction of Acquisition of Ball and Roller Bearings 252.225-7016
Restriction on Acquisition of Foreign Anchor and Mooring Chain 252.225-7019
Trade Agreements Certificate 252.225-7020
Trade Agreements 252.227-7021
Restriction on Acquisition of Forgings 252.225-7025
Restriction on Contingent Fees for Foreign Military Sales 252.225-7027
Exclusionary Policies and Practices of Foreign Governments 252.225-7028
Restriction of Acquisition of Carbon, Alloy and Armor Steel Plate 252.225-7030
Secondary Arab Boycott of Israel 252.225-7031
Buy American Act – Free Trade Agreements- Balance of Payments Program 252.225-7036
Restriction on Acquisition of Air Circuit Breakers 252.225-7038
Contractor Personnel Supporting U.S. Armed Forces Deployed Outside the United States 252.225-7040
Anti-terrorism/Force Protection for Defense Contractors Outside the United States 252.225-7043
Export Controlled Items 252.225-7048
Utilization of Indian Organizations, Indian-Owned Economic Enterprises, and Native Hawaiian Small Business Concerns
252.226-7001
Rights in Technical Data – Noncommercial items 252.227-7013
Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation 252.227-7014
Technical Data – Commercial Items 252.227-7015
Rights in Bid or Proposal Information (No substitutions for “Government” or “Contracting Officer” are made) 252.227-7016
Identification and Assertion of Use, Release or Disclosure Restrictions 252.227-7017
Rights in Noncommercial Technical Data and Computer Software – Small Business Innovation Research (SBIR) Program
252.227-7018
Validation of Asserted Restrictions – Computer Software 252.227-7019
Rights in Special Works 252.227-7020
Rights in Data – Existing Works 252.227-7021
Limitation on the Use or Disclosure of Government-Furnished Information Marked with Restrictive Legends (No substitution is made for “Government”) 252.227-7025
Deferred Delivery of Technical Data or Computer Software 252.227-7026
Deferred Ordering of Technical Data or Computer Software 252.227-7027
Technical Data or Computer Software Previously Delivered to the Government 252.227-7028
Technical Data – Withholding of Payment 252.227-7030
Rights In Shop Drawings 252.227-7033
Validation of Restrictive Markings on Technical Data 252.227-7037
Patent Rights Ownership by Contractor (Large Business) 252.227-7038
Patents – Reporting of Subject Inventions 252.227-7039
Status of Contractor as Direct Contractor (Spain) 252.229-7004

Reporting of Foreign Taxes – US Assistance 252.229-7011
Supplemental Cost Principles 252.231-7000
Frequency Authorization 252.235-7003
Modification Proposals – Price Breakdown 252.236-7000
Cloud Computing Services 252.239-7010
Telecommunications Security Equipment, Devices, Techniques and Services 252.239-7016
Pricing of Contract Modifications 252.243-7001
Subcontracts for Commercial Items and Commercial Components 252.244-7000
Warranty of Data 252.246-7001
Notification of Potential Safety Issues 252.246-7003
Pass-Through of Motor Carrier Fuel Surcharge Adjustment to the Cost Bearer 252.247-7003
Contractor Counterfeit Electronic Part Detection and Avoidance System 252.246-7007
Representation of Extent of Transportation by Sea 252.247-7022
Transportation of Supplies by Sea 252.247-7023
Notification of Transportation of Supplies by Sea 252.247-7024

Orders Over $100,000 Shall Also Include the Following:
Prohibition on Persons Convicted of Fraud or Other Defense Contract Related Felonies 252.203-7001
Transportation of Supplies by Sea 252.247-7023
Notification of Anticipated Contract Terminations or Reductions 252.249-7002

Orders Over $650,000 Shall Also Include the Following:
Small, Business Subcontracting Plan (DOD Contracts) 252.219-7003

Orders Over $700,000 Shall Also Include the Following:
Reporting of Contract Performance Outside the United States and Canada – Submission after Award (first tier subcontractors only) 252.225-7004

Orders Over $1,000,000 Shall Also Include the Following:
Acquisition Streamlining 252.211-7000
Waiver of United Kingdom Levies 252.225-7033

Orders Performed Outside the United States:
Contractor Personnel Authorized to Accompany U.S. Forces Deployed Outside the United States 252.225-7040

FAR and DFARS Clauses Required to be Flowed Down on all Subcontracts in their Entirety

DFARS 252.225-7007 Prohibition on Acquisition of Certain Items from Communist Chinese Military Companies.
As prescribed in 225.1103(4), use the following clause:
PROHIBITION ON ACQUISITION OF CERTAIN ITEMS FROM COMMUNIST CHINESE MILITARY COMPANIES (DEC 2018)
(a) Definitions. As used in this clause—
"600 series of the Commerce Control List" means the series of 5-character export control classification numbers (ECCNs) of the Commerce Control List of the Export Administration Regulations in 15 CFR part 774, supplement No. 1. that have a "6" as the third character. The 600 series constitutes the munitions and munitions-related ECCNs within the larger Commerce Control List. (See definition of "600 series" in 15 CFR 772.)
Communist Chinese military company" means any entity, regardless of geographic location that is—

(1) A part of the commercial or defense industrial base of the People's Republic of China including a subsidiary or affiliate of such entity; or

(2) Owned or controlled by, or affiliated with, an element of the Government or armed forces of the People's Republic of China.

"Item" means—

(1) A USML defense article, as defined at 22 CFR 120.6;

(2) A USML defense service, as defined at 22 CFR 120.9; or

(3) A 600 series item, as defined at 15 CFR 772.1.

"United States Munitions List" means the munitions list of the International Traffic in Arms Regulation in 22 CFR part 121.

(b) Any items covered by the United States Munitions List or the 600 series of the Commerce Control List that are delivered under this contract may not be acquired, directly or indirectly, from a Communist Chinese military company.

(c) The Contractor shall insert the substance of this clause, including this paragraph (c), in all subcontracts for items covered by the United States Munitions List or the 600 series of the Commerce Control List.

DFARS 252.204-7012 Safeguarding covered defense information and cyber incident reporting.
Safeguarding Covered Defense Information and Cyber Incident Reporting (DEC 2019)
(a) Definitions. As used in this clause -
Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.
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.
Contractor attributional/proprietary information means information that identifies the contractor(s), whether directly or indirectly, by the grouping of information that can be traced back to the contractor(s) (e.g., program description, facility locations), personally identifiable information, as well as trade secrets, commercial or financial information, or other commercially sensitive information that is not customarily shared outside of the company.
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 contractor information system means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.
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.
Forensic analysis means the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
Malicious software means computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes

a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.
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.
Operationally critical support means supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.
Rapidly report means within 72 hours of discovery of any cyber incident.
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) Adequate security. The Contractor shall provide adequate security on all covered contractor information systems. To provide adequate security, the Contractor shall implement, at a minimum, the following information security protections:
(1) For covered contractor information systems that are part of an information technology (IT) service or system operated on behalf of the Government, the following security requirements apply:
(i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.
(ii) Any other such IT service or system (i.e., other than cloud computing) shall be subject to the security requirements specified elsewhere in this contract.
(2) For covered contractor information systems that are not part of an IT service or system operated on behalf of the Government and therefore are not subject to the security requirement specified at paragraph (b)(1) of this clause, the following security requirements apply:
(i) Except as provided in paragraph (b)(2)(ii) of this clause, the covered contractor information system shall be subject to the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" (available via the internet at http://dx.doi.org/10.6028/NIST.SP.800-171) in effect at the time the solicitation is issued or as authorized by the Contracting Officer.
(ii)
(A) The Contractor shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the Contractor shall notify the DoD Chief Information Officer (CIO), via email at osd.dibcsia@mail.mil, within 30 days of contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.
(B) The Contractor shall submit requests to vary from NIST SP 800-171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place.
(C) If the DoD CIO has previously adjudicated the contractor's requests indicating that a requirement is not applicable or that an alternative security measure is equally effective, a copy of that approval shall be provided to the Contracting Officer when requesting its recognition under this contract.
(D) If the Contractor intends to use an external cloud service provider to store, process, or transmit any covered defense information in performance of this contract, the Contractor shall require and ensure that the cloud service provider meets security requirements equivalent to those established by the Government for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline (https://www.fedramp.gov/resources/documents/) and that the cloud service provider complies with requirements in paragraphs (c) through (g) of this clause for cyber incident reporting, malicious software, media preservation and

protection, access to additional information and equipment necessary for forensic analysis, and cyber incident damage assessment.
(3) Apply other information systems security measures when the Contractor reasonably determines that information systems security measures, in addition to those identified in paragraphs (b)(1) and (2) of this clause, may be required to provide adequate security in a dynamic environment or to accommodate special circumstances (e.g., medical devices) and any individual, isolated, or temporary deficiencies based on an assessed risk or vulnerability. These measures may be addressed in a system security plan.
(c) Cyber incident reporting requirement.
(1) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall -
(i) Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor's network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor's ability to provide operationally critical support; and
(ii) Rapidly report cyber incidents to DoD at https://dibnet.dod.mil.
(2) Cyber incident report. The cyber incident report shall be treated as information created by or for DoD and shall include, at a minimum, the required elements at https://dibnet.dod.mil.
(3) Medium assurance certificate requirement. In order to report cyber incidents in accordance with this clause, the Contractor or subcontractor shall have or acquire a DoD-approved medium assurance certificate to report cyber incidents. For information on obtaining a DoD-approved medium assurance certificate, see https://public.cyber.mil/eca/.
(d) Malicious software. When the Contractor or subcontractors discover and isolate malicious software in connection with a reported cyber incident, submit the malicious software to DoD Cyber Crime Center (DC3) in accordance with instructions provided by DC3 or the Contracting Officer. Do not send the malicious software to the Contracting Officer.
(e) Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.
(f) Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.
(g) Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.
(h) DoD safeguarding and use of contractor attributional/proprietary information. The Government shall protect against the unauthorized use or release of information obtained from the contractor (or derived from information obtained from the contractor) under this clause that includes contractor attributional/proprietary information, including such information submitted in accordance with paragraph (c). To the maximum extent practicable, the Contractor shall identify and mark attributional/proprietary information. In making an authorized release of such information, the Government will implement appropriate procedures to minimize the contractor attributional/proprietary information that is included in such authorized release, seeking to include only that information that is necessary for the authorized purpose(s) for which the information is being released.
(i) Use and release of contractor attributional/proprietary information not created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is not created by or for DoD is authorized to be released outside of DoD -
(1) To entities with missions that may be affected by such information;

(2) To entities that may be called upon to assist in the diagnosis, detection, or mitigation of cyber incidents;
(3) To Government entities that conduct counterintelligence or law enforcement investigations;
(4) For national security purposes, including cyber situational awareness and defense purposes (including with Defense Industrial Base (DIB) participants in the program at 32 CFR part 236); or
(5) To a support services contractor ("recipient") that is directly supporting Government activities under a contract that includes the clause at 252.204-7009, Limitations on the Use or Disclosure of Third-Party Contractor Reported Cyber Incident Information.
(j) Use and release of contractor attributional/proprietary information created by or for DoD. Information that is obtained from the contractor (or derived from information obtained from the contractor) under this clause that is created by or for DoD (including the information submitted pursuant to paragraph (c) of this clause) is authorized to be used and released outside of DoD for purposes and activities authorized by paragraph (i) of this clause, and for any other lawful Government purpose or activity, subject to all applicable statutory, regulatory, and policy based restrictions on the Government's use and release of such information.
(k) The Contractor shall conduct activities under this clause in accordance with applicable laws and regulations on the interception, monitoring, access, use, and disclosure of electronic communications and data.
(l) Other safeguarding or reporting requirements. The safeguarding and cyber incident reporting required by this clause in no way abrogates the Contractor's responsibility for other safeguarding or cyber incident reporting pertaining to its unclassified information systems as required by other applicable clauses of this contract, or as a result of other applicable U.S. Government statutory or regulatory requirements.
(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 252.225-7048 Export-Controlled items
(a) Definition. "Export-controlled items," as used in this clause, means items subject to the Export Administration Regulations (EAR) (15 CFR Parts 730-774) or the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130). The term includes -
(1) "Defense items," defined in the Arms Export Control Act, 22 U.S.C. 2778(j)(4)(A), as defense articles, defense services, and related technical data, and further defined in the ITAR, 22 CFR Part 120; and
(2) "Items," defined in the EAR as "commodities", "software", and "technology," terms that are also defined in the EAR, 15 CFR 772.1.
(b) The Contractor shall comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for contractors to register with the Department of State in accordance with the ITAR. The Contractor shall consult with the Department of State regarding any questions relating to compliance with the ITAR and shall consult with the Department of Commerce regarding any questions relating to compliance with the EAR.
(c) The Contractor's responsibility to comply with all applicable laws and regulations regarding export-controlled items exists independent of, and is not established or limited by, the information provided by this clause.
(d) Nothing in the terms of this contract adds, changes, supersedes, or waives any of the requirements of applicable Federal laws, Executive orders, and regulations, including but not limited to -
(1) The Export Administration Act of 1979, as amended (50 U.S.C. App. 2401, et seq.);
(2) The Arms Export Control Act (22 U.S.C. 2751, et seq.);
(3) The International Emergency Economic Powers Act (50 U.S.C. 1701, et seq.);

(4) The Export Administration Regulations (15 CFR Parts 730-774);
(5) The International Traffic in Arms Regulations (22 CFR Parts 120-130); and
(6) Executive Order 13222, as extended.
(e) The Contractor shall include the substance of this clause, including this paragraph (e), in all subcontracts.