Contract Clauses in this section are from the FAR, Defense FAR Sup, Air Force FAR Sup, and the Air Force Materiel Command FAR Sup, and are current through the following updates:

Database_Version: 7.3.x.1600; Issued: 12/3/2019; FAR: FAC 2020-01; DFAR: DPN20191127; DL.: DL 98-021; Class Deviations: CD 2020-O0001; AFFAR: 2002 Edition; AFAC: AFAC 2017-1003; IPN: 98-009

I. NOTICE: The following contract clauses pertinent to this section are hereby incorporated by reference:

A. FEDERAL ACQUISITION REGULATION CONTRACT CLAUSES

52.202-01	DEFINITIONS (JUN 2020)
52.203-03	GRATUITIES (APR 1984)
52.203-05	COVENANT AGAINST CONTINGENT FEES (MAY 2014)
52.203-06	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT (JUN 2020)
52.203-06	RESTRICTIONS ON SUBCONTRACTOR SALES TO THE GOVERNMENT (JUN 2020) - ALTERNATE I (OCT 1995)
52.203-08	CANCELLATION, RESCISSION, AND RECOVERY OF FUNDS FOR ILLEGAL OR IMPROPER ACTIVITY (MAY 2014)
52.203-10	PRICE OR FEE ADJUSTMENT FOR ILLEGAL OR IMPROPER ACTIVITY (MAY 2014)
52.203-12	LIMITATION ON PAYMENTS TO INFLUENCE CERTAIN FEDERAL TRANSACTIONS (JUN 2020)
52.203-13	CONTRACTOR CODE OF BUSINESS ETHICS AND CONDUCT (JUN 2020)
52.203-17	CONTRACTOR EMPLOYEE WHISTLEBLOWER RIGHTS AND REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (JUN 2020)
52.203-19	PROHIBITION ON REQUIRING CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS OR STATEMENTS (JAN 2017)
52.204-04	PRINTED OR COPIED DOUBLE-SIDED ON POSTCONSUMER FIBER CONTENT PAPER (MAY 2011)
52.204-10	REPORTING EXECUTIVE COMPENSATION AND FIRST-TIER SUBCONTRACT AWARDS (JUN 2020)
52.204-12	UNIQUE ENTITY IDENTIFIER MAINTENANCE (OCT 2016)
52.204-13	SYSTEM FOR AWARD MANAGEMENT MAINTENANCE (OCT 2018)
52.204-14	SERVICE CONTRACT REPORTING REQUIREMENTS (OCT 2016)
52.204-18	COMMERCIAL AND GOVERNMENT ENTITY CODE MAINTENANCE (AUG 2020)
52.204-19	INCORPORATION BY REFERENCE OF REPRESENTATIONS AND CERTIFICATIONS (DEC 2014)
52.204-23	PROHIBITION ON CONTRACTING FOR HARDWARE, SOFTWARE, AND SERVICES DEVELOPED OR PROVIDED BY KASPERSKY LAB AND OTHER COVERED ENTITIES (JUL 2018)
52.204-25	PROHIBITION ON CONTRACTING FOR CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT (AUG 2020)
52.209-06	PROTECTING THE GOVERNMENT'S INTEREST WHEN SUBCONTRACTING WITH CONTRACTORS DEBARRED, SUSPENDED, OR PROPOSED FOR DEBARMENT (JUN 2020)
52.209-10	PROHIBITION ON CONTRACTING WITH INVERTED DOMESTIC CORPORATIONS (NOV 2015)
52.212-04	CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (OCT 2018)
52.215-08	ORDER OF PRECEDENCE--UNIFORM CONTRACT FORMAT (OCT 1997)
52.215-10	PRICE REDUCTION FOR DEFECTIVE CERTIFIED COST OR PRICING DATA (AUG 2011)
52.215-12	SUBCONTRACTOR CERTIFIED COST OR PRICING DATA (JUN 2020)

52.215-12	SUBCONTRACTOR CERTIFIED COST OR PRICING DATA (DEVIATION 2018-O0015) (MAY 2018)
52.215-15	PENSION ADJUSTMENTS AND ASSET REVERSIONS (OCT 2010)
52.215-18	REVERSION OR ADJUSTMENT OF PLANS FOR POSTRETIREMENT BENEFITS (PRB) OTHER THAN PENSIONS (JUL 2005)
52.215-19	NOTIFICATION OF OWNERSHIP CHANGES (OCT 1997)
52.215-21	REQUIREMENTS FOR CERTIFIED COST OR PRICING DATA AND DATA OTHER THAN CERTIFIED COST OR PRICING DATA--MODIFICATIONS (JUN 2020)
52.215-23	LIMITATIONS ON PASS-THROUGH CHARGES (JUN 2020) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.216-07	ALLOWABLE COST AND PAYMENT (AUG 2018) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.216-08	FIXED FEE (JUN 2011) Applies to Cost-Plus-Fixed-Fee CLIN(s) only.
52.216-11	COST CONTRACT -- NO FEE (APR 1984) Applies to Cost CLIN(s) only.
52.217-08	OPTION TO EXTEND SERVICES (NOV 1999) Period of time. '30 days'
52.219-08	UTILIZATION OF SMALL BUSINESS CONCERNS (OCT 2018)
52.219-09	SMALL BUSINESS SUBCONTRACTING PLAN (JUN 2020)
52.219-09	SMALL BUSINESS SUBCONTRACTING PLAN (DEVIATION 2018-O0018) (AUG 2018)
52.219-28	POST-AWARD SMALL BUSINESS PROGRAM REREPRESENTATION (MAY 2020) - ALTERNATE I (MAR 2020) Para (h)(1), NAICS codes '334511'
52.222-02	PAYMENT FOR OVERTIME PREMIUMS (JUL 1990) Para (a), Dollar amount is 'zero' Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.222-03	CONVICT LABOR (JUN 2003)
52.222-19	CHILD LABOR--COOPERATION WITH AUTHORITIES AND REMEDIES (JAN 2020)
52.222-19	CHILD LABOR--COOPERATION WITH AUTHORITIES AND REMEDIES (DEVIATION 2020-O0019) (JUL 2020)
52.222-21	PROHIBITION OF SEGREGATED FACILITIES (APR 2015)
52.222-26	EQUAL OPPORTUNITY (SEP 2016)
52.222-29	NOTIFICATION OF VISA DENIAL (APR 2015)
52.222-35	EQUAL OPPORTUNITY FOR VETERANS (JUN 2020)
52.222-36	EQUAL OPPORTUNITY FOR WORKERS WITH DISABILITIES (JUN 2020)
52.222-37	EMPLOYMENT REPORTS ON VETERANS (JUN 2020)
52.222-40	NOTIFICATION OF EMPLOYEE RIGHTS UNDER THE NATIONAL LABOR RELATIONS ACT (DEC 2010)
52.222-50	COMBATING TRAFFICKING IN PERSONS (JAN 2019)
52.223-06	DRUG-FREE WORKPLACE (MAY 2001)
52.223-18	ENCOURAGING CONTRACTOR POLICIES TO BAN TEXT MESSAGING WHILE DRIVING (JUN 2020)
52.225-13	RESTRICTIONS ON CERTAIN FOREIGN PURCHASES (JUN 2008)
52.225-14	INCONSISTENCY BETWEEN ENGLISH VERSION AND TRANSLATION OF CONTRACT (FEB 2000)
52.227-01	AUTHORIZATION AND CONSENT (JUN 2020)
52.227-02	NOTICE AND ASSISTANCE REGARDING PATENT AND COPYRIGHT INFRINGEMENT (JUN 2020)
52.227-21	TECHNICAL DATA DECLARATION, REVISION, AND WITHHOLDING OF PAYMENT - MAJOR SYSTEMS (MAY 2014)
52.228-07	INSURANCE -- LIABILITY TO THIRD PERSONS (MAR 1996) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.229-04	FEDERAL, STATE, AND LOCAL TAXES (STATE AND LOCAL ADJUSTMENTS) (FEB 2013) Applies to Firm-Fixed-Price CLIN(s) only.

52.230-02	COST ACCOUNTING STANDARDS (JUN 2020)
52.230-02	COST ACCOUNTING STANDARDS (DEVIATION 2018-O0015) (MAY 2018)
52.230-06	ADMINISTRATION OF COST ACCOUNTING STANDARDS (JUN 2010)
52.232-01	PAYMENTS (APR 1984) Applies to Firm-Fixed-Price CLIN(s) only.
52.232-08	DISCOUNTS FOR PROMPT PAYMENT (FEB 2002) Applies to Firm-Fixed-Price CLIN(s) only.
52.232-11	EXTRAS (APR 1984) Applies to Firm-Fixed-Price CLIN(s) only.
52.232-17	INTEREST (MAY 2014)
52.232-20	LIMITATION OF COST (APR 1984) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.232-23	ASSIGNMENT OF CLAIMS (MAY 2014)
52.232-33	PAYMENT BY ELECTRONIC FUNDS TRANSFER - SYSTEM FOR AWARD MANAGEMENT (OCT 2018)
52.232-39	UNENFORCEABILITY OF UNAUTHORIZED OBLIGATIONS (JUN 2013)
52.232-40	PROVIDING ACCELERATED PAYMENTS TO SMALL BUSINESS SUBCONTRACTORS (DEC 2013)
52.233-01	DISPUTES (MAY 2014)
52.233-03	PROTEST AFTER AWARD (AUG 1996) Applies to Firm-Fixed-Price CLIN(s) only.
52.233-03	PROTEST AFTER AWARD (AUG 1996) - ALTERNATE I (JUN 1985) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.233-04	APPLICABLE LAW FOR BREACH OF CONTRACT CLAIM (OCT 2004)
52.234-01	INDUSTRIAL RESOURCES DEVELOPED UNDER TITLE III, DEFENSE PRODUCTION ACT (SEP 2016)
52.242-01	NOTICE OF INTENT TO DISALLOW COSTS (APR 1984) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.242-03	PENALTIES FOR UNALLOWABLE COSTS (MAY 2014) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.242-13	BANKRUPTCY (JUL 1995)
52.243-01	CHANGES -- FIXED-PRICE (AUG 1987) Applies to Firm-Fixed-Price CLIN(s) only.
52.243-01	CHANGES -- FIXED-PRICE (AUG 1987) - ALTERNATE II (APR 1984) Applies to Firm-Fixed-Price CLIN(s) only.
52.243-02	CHANGES -- COST-REIMBURSEMENT (AUG 1987) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.243-02	CHANGES -- COST-REIMBURSEMENT (AUG 1987) - ALTERNATE II (APR 1984) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.243-07	NOTIFICATION OF CHANGES (JAN 2017) Para (b), Number of calendar days is (insert 30 for RDSS/C) '30 days' Para (d), Number of calendar days is (insert 30 for RDSS/C) '30 days'
52.244-02	SUBCONTRACTS (JUN 2020) Para (d), approval required on subcontracts: 'N/A' Para (j), Insert subcontracts evaluated during negotiations. 'N/A' Applies to Firm-Fixed-Price CLIN(s) only.
52.244-02	SUBCONTRACTS (JUN 2020) - ALTERNATE I (JUN 2020) Para (d), Contractor shall obtain the Contracting Officer's written consent before placing the following subcontracts: 'N/A' Para (j), the following subcontracts which were evaluated during negotiations: 'N/A' Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.245-01	GOVERNMENT PROPERTY (JAN 2017) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.245-09	USE AND CHARGES (APR 2012) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.

52.246-24 LIMITATION OF LIABILITY -- HIGH-VALUE ITEMS (FEB 1997) - ALTERNATE I (APR 1984)
52.246-25 LIMITATION OF LIABILITY -- SERVICES (FEB 1997)
52.247-01 COMMERCIAL BILL OF LADING NOTATIONS (FEB 2006)
52.248-01 VALUE ENGINEERING (JUN 2020)
Para (m). Contract number. 'FA8615-21-C-6050'
52.248-02 VALUE ENGINEERING -- ARCHITECT-ENGINEER (MAR 1990)
52.249-02 TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (FIXED-PRICE) (APR 2012)
Applies to Firm-Fixed-Price CLIN(s) only.
52.249-03 TERMINATION FOR CONVENIENCE OF THE GOVERNMENT (DISMANTLING, DEMOLITION, OR REMOVAL OF IMPROVEMENTS) (APR 2012)
52.249-06 TERMINATION (COST-REIMBURSEMENT) (MAY 2004)
Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.249-08 DEFAULT (FIXED-PRICE SUPPLY AND SERVICE) (APR 1984)
Applies to Firm-Fixed-Price CLIN(s) only.
52.249-14 EXCUSABLE DELAYS (APR 1984)
Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
52.253-01 COMPUTER GENERATED FORMS (JAN 1991)

B. DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT CONTRACT CLAUSES

252.203-7000 REQUIREMENTS RELATING TO COMPENSATION OF FORMER DOD OFFICIALS (SEP 2011)
252.203-7002 REQUIREMENT TO INFORM EMPLOYEES OF WHISTLEBLOWER RIGHTS (SEP 2013)
252.203-7003 AGENCY OFFICE OF THE INSPECTOR GENERAL (AUG 2019)
252.203-7004 DISPLAY OF HOTLINE POSTERS (AUG 2019)
252.204-7000 DISCLOSURE OF INFORMATION (OCT 2016)
252.204-7003 CONTROL OF GOVERNMENT PERSONNEL WORK PRODUCT (APR 1992)
252.204-7015 NOTICE OF AUTHORIZED DISCLOSURE OF INFORMATION TO LITIGATION SUPPORT (MAY 2016)
252.204-7018 PROHIBITION ON THE ACQUISITION OF COVERED DEFENSE TELECOMMUNICATIONS EQUIPMENT OR SERVICES (DEC 2019)
252.204-7020 NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (NOV 2020)
252.205-7000 PROVISION OF INFORMATION TO COOPERATIVE AGREEMENT HOLDERS (DEC 1991)
252.209-7004 SUBCONTRACTING WITH FIRMS THAT ARE OWNED OR CONTROLLED BY THE GOVERNMENT OF A COUNTRY THAT IS A STATE SPONSOR OF TERRORISM (MAY 2019)
252.211-7003 ITEM UNIQUE IDENTIFICATION AND VALUATION (MAR 2016)
Para (c)(1)(i). Insert Contract Line, Subline, or Exhibit Line Item Number and Item Description or n/a. 'N/A'
Para (c)(1)(ii). Identify Contract Line, Subline, or Exhibit Line Item Nr and Item Description. If items are identified in the Schedule, insert "See Schedule" 'N/A'
Para (c)(1)(iii). Attachment Nr. 'N/A'
Para (c)(1)(iv). Attachment Nr. 'N/A'
Para (f)(2)(iii). Line item number or n/a. 'N/A'
252.211-7007 REPORTING OF GOVERNMENT-FURNISHED PROPERTY (AUG 2012)
Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
252.211-7008 USE OF GOVERNMENT-ASSIGNED SERIAL NUMBERS (SEP 2010)
252.215-7002 COST ESTIMATING SYSTEM REQUIREMENTS (DEC 2012)
252.215-7015 PROGRAM SHOULD-COST REVIEW (NOV 2019)
252.217-7000 EXERCISE OF OPTION TO FULFILL FOREIGN MILITARY SALES COMMITMENTS - BASIC (NOV 2014)

	Para (b), Name of country 'Taipei Economic and Cultural Representative Office in the United States'
	Para (b), Applicable CLIN '1001, 1002, 1003, 1004, 1005, 1006, and 1007'
252.219-7003	SMALL BUSINESS SUBCONTRACTING PLAN (DOD CONTRACTS) -- BASIC (DEC 2019)
252.225-7001	BUY AMERICAN AND BALANCE OF PAYMENTS PROGRAM - BASIC (DEC 2017)
252.225-7002	QUALIFYING COUNTRY SOURCES AS SUBCONTRACTORS (DEC 2017)
252.225-7008	RESTRICTION ON ACQUISITION OF SPECIALTY METALS (MAR 2013)
252.225-7009	RESTRICTION ON ACQUISITION OF CERTAIN ARTICLES CONTAINING SPECIALTY METALS (DEC 2019)
252.225-7012	PREFERENCE FOR CERTAIN DOMESTIC COMMODITIES (DEC 2017)
252.225-7048	EXPORT-CONTROLLED ITEMS (JUN 2013)
252.225-7052	RESTRICTION ON THE ACQUISITION OF CERTAIN MAGNETS, TANTALUM, AND TUNGSTEN (DEVIATION 2020-O0006) (FEB 2020)
252.226-7001	UTILIZATION OF INDIAN ORGANIZATIONS, INDIAN-OWNED ECONOMIC ENTERPRISES, AND NATIVE HAWAIIAN SMALL BUSINESS CONCERNS (APR 2019)
252.227-7015	TECHNICAL DATA--COMMERCIAL ITEMS (FEB 2014)
252.227-7037	VALIDATION OF RESTRICTIVE MARKINGS ON TECHNICAL DATA (SEP 2016)
252.231-7000	SUPPLEMENTAL COST PRINCIPLES (DEC 1991)
252.232-7003	ELECTRONIC SUBMISSION OF PAYMENT REQUESTS AND RECEIVING REPORTS (DEC 2018)
252.232-7010	LEVIES ON CONTRACT PAYMENTS (DEC 2006)
252.237-7010	PROHIBITION ON INTERROGATION OF DETAINEES BY CONTRACTOR PERSONNEL (JUN 2013)
252.239-7018	SUPPLY CHAIN RISK (FEB 2019)
252.242-7005	CONTRACTOR BUSINESS SYSTEMS (FEB 2012)
252.242-7006	ACCOUNTING SYSTEM ADMINISTRATION (FEB 2012) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
252.243-7001	PRICING OF CONTRACT MODIFICATIONS (DEC 1991) Applies to Firm-Fixed-Price CLIN(s) only.
252.243-7002	REQUESTS FOR EQUITABLE ADJUSTMENT (DEC 2012)
252.244-7000	SUBCONTRACTS FOR COMMERCIAL ITEMS (JUN 2013)
252.244-7001	CONTRACTOR PURCHASING SYSTEM ADMINISTRATION - BASIC (MAY 2014) Applies to Firm-Fixed-Price CLIN(s) only.
252.244-7001	CONTRACTOR PURCHASING SYSTEM ADMINISTRATION - ALTERNATE I (MAY 2014) - ALTERNATE I (MAY 2014) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
252.245-7001	TAGGING, LABELING, AND MARKING OF GOVERNMENT-FURNISHED PROPERTY (APR 2012) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
252.245-7002	REPORTING LOSS OF GOVERNMENT PROPERTY (DEVIATION 2020-O0004) (FEB 2020) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
252.245-7003	CONTRACTOR PROPERTY MANAGEMENT SYSTEM ADMINISTRATION (APR 2012) Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
252.245-7004	REPORTING, REUTILIZATION, AND DISPOSAL (DEC 2017) Insert Item(s) 'N/A' Insert Item(s) 'N/A' Applies to Cost-Plus-Fixed-Fee CLIN(s), Cost CLIN(s) only.
252.246-7003	NOTIFICATION OF POTENTIAL SAFETY ISSUES (JUN 2013)
252.246-7007	CONTRACTOR COUNTERFEIT ELECTRONIC PART DETECTION AND AVOIDANCE SYSTEM (AUG 2016)
252.246-7008	SOURCES OF ELECTRONIC PARTS (MAY 2018)
252.247-7023	TRANSPORTATION OF SUPPLIES BY SEA - BASIC (FEB 2019)
252.247-7028	APPLICATION FOR U.S. GOVERNMENT SHIPPING DOCUMENTATION/INSTRUCTIONS (JUN 2012)

252.249-7002 NOTIFICATION OF ANTICIPATED CONTRACT TERMINATION OR REDUCTION (JUN 2020)

C. AIR FORCE FEDERAL ACQUISITION REGULATION SUPPLEMENT CONTRACT CLAUSES

5352.201-9101 OMBUDSMAN (OCT 2019)
Para (c). Ombudsmen names, addresses, phone numbers, fax, and email addresses. 'Major Randall Mullen, Deputy Chief of Contracts, Helicopter Program Office, AFLCMC/WIS, 937-257-8984, Randall.Mullen.1@us.af.mil'
5352.223-9000 ELIMINATION OF USE OF CLASS I OZONE DEPLETING SUBSTANCES (ODS) (OCT 2019)

II. NOTICE: The following contract clauses pertinent to this section are hereby incorporated in full text:

FEDERAL ACQUISITION REGULATION CONTRACT CLAUSES IN FULL TEXT

52.204-21 BASIC SAFEGUARDING OF COVERED CONTRACTOR INFORMATION SYSTEMS (JUN 2016)

(a) Definitions. As used in this clause--

Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal contract information.

Federal contract information means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.

Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).

Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).

Safeguarding means measures or controls that are prescribed to protect information systems.

(b) Safeguarding requirements and procedures.

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

(2) Other requirements. This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

(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.

52.212-04 ADDENDUM TO CONTRACT TERMS AND CONDITIONS--COMMERCIAL ITEMS (DEC 2014)

52.212-4, Contract Terms and Conditions -- Commercial Items is hereby tailored as follows:

(a) The place of inspection, acceptance, and FOB is Inspection/Acceptance: Source .

FOB: Destination

52.217-07 OPTION FOR INCREASED QUANTITY -- SEPARATELY PRICED LINE ITEM (MAR 1989) (TAILORED)

The Government may require the delivery of the numbered line item, identified in the Schedule as an option item, in the quantity and at the price stated in the Schedule. The Contracting Officer may exercise

the option by written notice to the Contractor within 30 days. An exception is made for the first option to which in order to finalize the terms of the offset agreement, the Contractor will receive written notification of the Government's intent to exercise the option(s) 6 months in advance. Delivery of added items shall continue at the same rate that like items are called for under the contract, unless the parties otherwise agree.

The inclusion of an offset shall be required at the time which the total contract value, including exercised options, results in a total obligation value of $5M or greater. Upon completion of the offset agreement, the parties shall modify the contract to include the price of the offset.

52.252-02 CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

https://www.acquisition.gov/browse/index/far
https://www.acquisition.gov/dfars
https://www.acquisition.gov/affars

52.252-06 AUTHORIZED DEVIATIONS IN CLAUSES (APR 1984)

(a) The use in this solicitation or contract of any Federal Acquisition Regulation (48 CFR Chapter 1) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the date of the clause.

(b) The use in this solicitation or contract of any Defense Federal Acquisition Regulation Supplement (48 CFR Chapter 2) clause with an authorized deviation is indicated by the addition of "(DEVIATION)" after the name of the regulation.

DEFENSE FAR SUPP CONTRACT CLAUSES IN FULL TEXT

252.204-7012 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.

"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.

"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 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 of 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 contrac, 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.